InterCERT FRANCE

RAPPORT ANNUEL

Étude sur les Risques Psychosociaux dans les CERTs

TLP:CLEAR

2025

Table des matières

Préface 5

Exec. summary 6

Étude sur les Risques Psychosociaux (RPS) dans les CERTs 10

Contexte et objectifs 10
Méthodologie 10
Profils et métiers 10
Données issues de l'étude InterCERT 11
Enseignements transversaux 11
Recommandations 12
Pistes complémentaires à développer 12
Conclusion 13

Présentation de l'InterCERT France 14

Description des CERTs 15

Cert Interne 15
Cert Externe 15
Cert Institutionnel 15

Présentation des métiers des CERTs/CSIRTs, SOC 16

Membres du Groupe de travail RPS 18

Méthodologie 21

Mode de recueil et périmètre de l'étude 22

Présentation des résultats 24

Conclusion 27

Facteurs de stress 28

Gestion du stress 28

Sources de Stress 29

Contenus psychologiquement difficiles 31
Problématiques éthiques 32
Sur-sollicitations en période d'incident 33
Dispositifs de crise 34
Implication de ressources personnelles 35

Cadre contractuel 36

Horaires de travail 36
Prise en compte des Risques Psycho Sociaux dans l'Entreprise 37
Aspects contractuels 39
Les moteurs des répondants 40

Préconisations et pistes d'action/Prise en charge des RPS par l'employeur 42

Réaction et prise en charge individuelle 42
Réflexion organisationnelle 44

Conclusion 46

PRÉFACE

La cybersécurité est un domaine exigeant, mêlant expertise, forts enjeux et imprévu. Derrière les outils, les protocoles et les procédures, il y a des femmes et des hommes qui veillent, souvent dans l'ombre, à la sécurité numérique de nos organisations.

Après avoir présidé InterCERT France, j'ai perçu la hauteur de leur engagement et notre responsabilité à devoir les soutenir.

C'est pourquoi nous avons lancé en 2024 une étude inédite sur les risques psychosociaux (RPS) au sein des équipes CERT et SOC. Près de 250 professionnels ont participé à cette enquête, apportant une parole précieuse, parfois difficile, mais toujours lucide.

Les résultats sont sans appel : charge émotionnelle, sous-valorisation du travail accomplie, culture du « tout-urgence », difficulté à déconnecter… autant de facteurs qui fragilisent nos équipes et appellent à une action collective.

Cette étude s'inscrit pleinement dans les missions de l'InterCERT France : fédérer les équipes de la réponse à incidents, promouvoir les bonnes pratiques, renforcer la coopération entre entités publiques et privées, et surtout, soutenir les professionnels dans leur quotidien.

Elle met en lumière une réalité souvent tue, dans une communauté majoritairement masculine où l'expression du stress ou de la vulnérabilité reste encore taboue.

Pourtant, parler des RPS, c'est reconnaître que la performance durable passe par le respect de l'humain. C'est affirmer que la parole, le soutien et la reconnaissance sont des piliers de notre résilience collective.

Ce Livre Blanc est un point de départ. Il propose des recommandations concrètes, applicables, et adaptées aux spécificités de nos métiers. Il appelle les directions, les managers, les institutions et chaque membre de notre réseau à se mobiliser. Car prendre soin des équipes, c'est aussi renforcer notre capacité à faire face aux crises, à protéger les systèmes, à servir l'intérêt général.

Je tiens à remercier chaleureusement tous les contributeurs, les répondants, et celles et ceux qui ont permis la réalisation de ce travail.

Que ce document inspire des actions durables, des transformations concrètes, et surtout, une reconnaissance pleine et entière de celles et ceux qui font la cybersécurité au quotidien.

Frédéric Le Bastard, Membre honoraire d'InterCERT France

EXEC. SUMMARY

En 2024, l'InterCERT France a réalisé la première étude dédiée aux risques psychosociaux (RPS) auprès des équipes CERT et SOC, impliquant près de 1 000 membres issus de différentes entités et différents profils. Cette initiative vise à mesurer la prévalence et l'intensité des RPS, à identifier les principaux facteurs de risque et à formuler des recommandations concrètes pour renforcer la qualité de vie au travail et la résilience des équipes, dans un contexte de pression croissante liée à la cybersécurité.

Trois enseignements clés :

01 **Les équipes CERT et SOC font face à une charge émotionnelle élevée**, générée par la gestion continue d'incidents critiques et la nécessité d'une vigilance permanente. D'après l'étude, **32,2% des répondants** identifient la **charge de travail** comme leur principale source de stress, et **35,7%** citent l'**impact des incidents** comme facteur de stress majeur pendant leur gestion. Cette pression favorise l'apparition de stress chronique et de troubles liés au surmenage.

02 **Le manque de reconnaissance et de valorisation du travail accompl**i ressort comme un facteur aggravant des RPS. Bien que **80% des répondants** considèrent que l'entreprise **prend en compte les risques psychosociaux, 72% jugent les moyens mis en œuvre insuffisants**, et **56%** estiment que l'approche RH est **trop générique**, ne répondant pas aux spécificités de leurs métiers. Ces chiffres traduisent un besoin fort de **visibilité accrue** des actions menées et d'un **soutien plus affirmé** de la part de la direction et des managers.

03 **La culture du "tout-urgence" et la difficulté à déconnecter** en dehors des horaires de travail accentuent le risque d'épuisement professionnel. Les métiers de la réponse sur incident, notamment au sein des CERT et SOC, sont particulièrement exposés à des **rythmes irréguliers : 18,9% des répondants** identifient ce facteur comme une source importante de stress. Ce contexte, combiné aux astreintes et horaires décalés, contribue à une fatigue accumulée et à une altération progressive de la qualité de vie au travail.

Cette étude met en lumière l'importance d'une approche proactive et collective pour prévenir les RPS au sein des équipes CERT et SOC. La mise en œuvre coordonnée de ces recommandations contribuera à renforcer l'engagement, la performance et la résilience des professionnels face aux défis croissants de la cybersécurité.

ÉTUDE SUR LES RISQUES PSYCHOSOCIAUX (RPS) DANS LES CERTS

CONTEXTE ET OBJECTIFS

En 2024, InterCERT France a mené la première étude nationale dédiée aux risques psychosociaux (RPS) auprès des équipes CERT et SOC. Près de 1000 professionnels ont participé à cette enquête : responsables CERT, analystes SOC, managers, issus d'entités variées.

Cette initiative vise à :

- Mesurer la prévalence et l'intensité des RPS selon les profils.
- Identifier les principaux facteurs de vulnérabilité.
- Proposer des recommandations concrètes pour améliorer la qualité de vie au travail et renforcer la résilience des équipes.

MÉTHODOLOGIE

Période	Septembre / 30 octobre 2024
Outil	Plateforme Sphinx
Questionnaire	Données sociodémographiques Échelles RPS standardisées Questions ouvertes
Confidentialité	Participation volontaire et anonyme ; résultats analysés uniquement sous forme agrégée

PROFILS ET MÉTIERS

Âge	68 % ont entre 30 et 45 ans, cœur opérationnel des CERTs 0,3 % ont moins de 25 ans, signalant un déficit de relève générationnelle 33 % ont plus de 45 ans, avec une expérience valorisable mais exposés à une usure cumulative
Sexe	Panel reflétant le marché de la cybersécurité, avec 18 % de femmes
Taille des équipes CERT/SOC	12,5 % très petites équipes (1–5 personnes) 39,5 % petites équipes (6–10 personnes) 31,8 % équipes moyennes (20–50 personnes) 17,2 % grandes équipes (>50 personnes)

TLP:CLEAR

DONNÉES ISSUES DE L'ÉTUDE INTERCERT

La majorité des CERTs en France fonctionnent en structures réduites ou moyennes, souvent sous contrainte de ressources humaines limitées.

- **Métiers étudiés :** Responsable SOC, Analyste SOC, Responsable CSIRT, Analyste réponse incidents, Gestionnaire de crise, Analyste CTI
- **Types de CERTs** : Interne, Externe, Institutionnel

Facteur	Observation	Commentaire
Gestion du stress	1/6 se sent préparé ; progression avec l'âge	L'expérience accroît la résilience, mais surcharge critique des 30–45 ans
Contenus difficiles	86 % exposés ; 1/5 quotidiennement	Besoin d'un suivi spécifique et d'un encadrement de l'exposition
Problématiques éthiques	50 % exposés d'avantage que rarement	Importance d'un cadre clair et de sensibilisation
Sur-sollicitations	50 % touchés ; moins fréquent dans grandes équipes	Nécessité d'organiser les interactions et bulles de protection
Débordements émotionnels	1/2 observés	Former les managers et instaurer des rituels de débrief post-incident et en cours de crise, pour prendre du recul et faire baisser la pression
Ressources personnelles	43 % utilisent leurs propres outils	Risques techniques et juridiques ; besoin d'un cadre et d'une sensibilisation
Cadre contractuel	50 % méconnaissent leurs droits et protections	Urgence de clarifier les contrats et d'informer les collaborateurs

ENSEIGNEMENTS TRANSVERSAUX

1. **Concentration générationnelle :** surcharge critique des 30–45 ans, quasi-absence de relève <25 ans, seniors à protéger et valoriser
2. **Taille des équipes comme facteur clé :**
   - Plus l'équipe est petite, plus la vulnérabilité aux RPS est forte (pas de relais, isolement, surcharge)
   - Les grandes équipes offrent plus de résilience (rotation, soutien mutuel), mais nécessitent des mécanismes de coordination robustes
3. **Exposition intense** aux contenus difficiles et aux sollicitations multiples
4. **Préparation inégale :** la résilience croît avec l'âge, mais le soutien organisationnel reste insuffisant
5. **Cadre juridique et RH lacunaire**, créant insécurité et méconnaissance des droits
6. **Culture de prévention fragmentée**, sans cadre commun structuré entre CERTs

TLP:CLEAR

RECOMMANDATIONS

À l'échelle individuelle

- Accès confidentiel à un accompagnement psychologique
- Formation à la gestion du stress et aux signaux faibles
- Espaces d'échange et rituels de débrief après incidents critiques

À l'échelle organisationnelle

- Clarifier les cadres contractuels (durée de travail et de repos, exposition aux données sensibles)
- Répartir équitablement les charges et assurer un suivi des incidents
- Former les managers comme « absorbeurs de stress »
- Instaurer des rituels collectifs post-incident et renforcer la cohésion d'équipe
- Mettre en place un tableau de bord RPS pour un suivi régulier par âge, fonction et taille de CERT

PISTES COMPLÉMENTAIRES À DÉVELOPPER

01 Suivi renforcé des collaborateurs exposés aux contenus sensibles

- Identifier les missions à forte charge émotionnelle et formaliser un protocole de suivi
- Proposer un accompagnement systématique post-incident (psychologue, cellule de soutien)
- Créer un registre confidentiel des expositions critiques pour assurer un suivi longitudinal

02 Encadrement de l'usage d'outils personnels

- Sensibiliser aux risques techniques, juridiques et psychologiques liés à l'usage d'outils non fournis
- Fournir des alternatives professionnelles adaptées à un usage CERT/SOC
- Intégrer des clauses claires dans les chartes informatiques et les contrats de mission

03 Indicateurs d'efficacité des actions RPS

- Définir des KPIs RPS : turnover, absentéisme, incidents critiques, recours aux dispositifs de soutien
- Mettre en place un tableau de bord partagé avec les RH et les directions opérationnelles
- Réaliser des bilans annuels RPS avec retour d'expérience des équipes

04 Développement d'une culture de la parole et du soutien

- Former les managers à l'écoute active et à la détection des signaux faibles
- Créer des espaces de parole réguliers (groupes de discussion, cafés RPS, forums internes)
- Valoriser les témoignages pour briser les tabous, notamment dans une communauté majoritairement masculine

05 Prévention ciblée selon les profils

- Adapter les dispositifs selon l'âge, la fonction et la taille de l'équipe
- Identifier les profils à risque et proposer des parcours de prévention personnalisés

06 Intégration des RPS dans les audits et les revues de sécurité

- Ajouter un volet RPS dans les audits internes des CERTs
- Intégrer les enjeux humains dans les revues post-incident et les exercices de crise
- Associer les référents RPS aux comités de pilotage cyber

CONCLUSION

Cette première étude met en évidence une communauté hautement exposée aux risques psychosociaux, avec :

- Une surcharge critique de la tranche 30-45 ans
- Une quasi-absence de relève générationnelle
- Une vulnérabilité accrue dans les petites équipes CERT/SOC

Les dispositifs actuels de prévention et de soutien sont fragmentés et insuffisamment adaptés au contexte cyber.

La mise en œuvre d'actions coordonnées, à la fois individuelles et organisationnelles, constitue un enjeu stratégique pour :

- Préserver la santé des équipes
- Garantir l'attractivité du métier
- Assurer la résilience collective face aux crises cyber.

PRÉSENTATION DE L'INTERCERT FRANCE

InterCERT France est l'association qui fédère les équipes de réponse à incidents de sécurité informatique (CSIRT, CERT et SOC) opérant en France, qu'elles soient issues du secteur public, privé ou académique. Créée pour favoriser la coopération et l'entraide en matière de cybersécurité, l'association regroupe aujourd'hui 120 membres.
Sa mission principale est de renforcer la résilience collective face aux cybermenaces.

En facilitant :

- Le partage d'informations sur les menaces et incidents,
- La mutualisation de bonnes pratiques opérationnelles (fiches réflexes, playbooks, étude d'incidentologie),
- Le développement de la confiance et de la solidarité entre les équipes de sécurité.

Au-delà de son rôle opérationnel, InterCERT France s'attache également à soutenir les professionnels de la cybersécurité. Consciente de la pression et du niveau de stress que peut générer la gestion d'incidents, l'association mène des travaux spécifiques sur les risques psychosociaux (RPS) dans le domaine cyber.

Ces initiatives visent à :

- Mieux comprendre l'impact humain des métiers de la réponse à incident,
- Sensibiliser les organisations aux enjeux de santé psychologique des équipes de cybersécurité,
- Proposer des pistes d'accompagnement pour prévenir le stress chronique, l'isolement ou l'épuisement professionnel.

En intégrant la dimension humaine au cœur de ses travaux, InterCERT France affirme sa volonté d'accompagner ses membres non seulement sur le plan technique, mais aussi sur celui de la santé et du bien-être au travail, condition indispensable pour une cybersécurité efficace et durable.

DESCRIPTION DES CERTS

Les CERT (Computer Emergency Response Teams), également appelés CSIRT (Computer Security Incident Response Teams), désignent des structures spécialisées dans la gestion des incidents de sécurité informatique. Le terme CERT est une marque déposée par le Software Engineering Institute (SEI) de l'université Carnegie Mellon, qui a créé le premier CERT en 1988 à la suite du ver Morris, marquant un tournant dans la coordination de la réponse aux incidents cyber.

Depuis, le modèle s'est largement diffusé à l'échelle internationale. Les CERTs et CSIRTs se déclinent aujourd'hui en plusieurs formes selon leur périmètre d'intervention (interne, sectoriel, institutionnel) et leur mission (détection, réponse, coordination, analyse). Ils constituent un maillon essentiel de la cybersécurité opérationnelle, en assurant la gestion des incidents, la veille sur les menaces, et le soutien aux entités confrontées à des crises cyber :

CERT INTERNE

Les CERT internes : ils sont créés au sein d'une organisation (entreprise, administration, groupe) pour protéger exclusivement son système d'information. Leur rôle est de détecter, analyser et traiter les incidents de sécurité qui concernent leur environnement propre. Ils travaillent en lien direct avec les équipes techniques et métiers internes, ce qui leur permet d'agir rapidement et de proposer des mesures adaptées aux spécificités de l'organisation.

CERT EXTERNE

Les CERT externes : ils proposent des services de réponse à incident à des clients tiers. Généralement portés par des prestataires spécialisés, ils interviennent sur demande pour accompagner des organisations dans la gestion d'incidents de cybersécurité. Leur valeur ajoutée réside dans l'expertise accumulée auprès d'un large éventail de clients et la capacité à mobiliser des ressources variées.

CERT INSTITUTIONNEL

Les CERT institutionnels : ils sont mis en place par des organismes publics ou para-publics, souvent avec une mission nationale ou sectorielle. Ils jouent un rôle de coordination, de veille et de soutien auprès des autres CERT ou des acteurs de leur périmètre (par exemple, un CERT national, sectoriel ou territorial). Ils contribuent à la diffusion de bonnes pratiques, à la circulation de l'information et au renforcement de la résilience collective.

PRÉSENTATION DES MÉTIERS DES CERTS/CSIRTS, SOC

La cybersécurité est aujourd'hui au cœur de la résilience des organisations. Les professionnels de la réponse à incident, qu'ils exercent au sein d'un CERT, CSIRT ou SOC, portent une responsabilité cruciale : détecter, analyser et contenir des attaques souvent complexes, parfois déstabilisantes, dans des délais extrêmement contraints.

Ces missions, essentielles à la continuité d'activité et à la protection des données, se caractérisent par **une forte intensité émotionnelle** et **cognitive** : gestion du stress, pression du temps, exposition à des menaces récurrentes, astreintes et nécessité d'une vigilance permanente. Cette réalité opérationnelle peut engendrer des risques psychosociaux (RPS), avec des impacts sur la santé psychologique des équipes, leur motivation et, in fine, leur efficacité collective.

À travers cette étude, InterCERT France a souhaité donner la parole aux professionnels du terrain afin de mieux comprendre les spécificités des métiers cyber face aux RPS, d'objectiver les difficultés rencontrées et d'identifier des leviers d'action concrets pour améliorer la prévention et l'accompagnement.

L'enjeu est double : protéger celles et ceux qui protègent nos systèmes d'information, et renforcer la capacité de nos organisations à faire face aux crises numériques dans la durée.:

Les CERT institutionnels : ils sont mis en place par des organismes publics ou para-publics, souvent avec une mission nationale ou sectorielle. Ils jouent un rôle de coordination, de veille et de soutien auprès des autres CERT ou des acteurs de leur périmètre (par exemple, un CERT national, sectoriel ou territorial). Ils contribuent à la diffusion de bonnes pratiques, à la circulation de l'information et au renforcement de la résilience collective.

https://cyber.gouv.fr/publications/panorama-des-metiers-de-la-cybersecurite

Responsable du SOC	Le responsable du SOC (Security Operation Center) planifie et organise les opérations quotidiennes du SOC afin d'évaluer le niveau de vulnérabilité et de détecter des activités suspectes ou malveillantes. Il met en place le service de détection des incidents de sécurité.Il valide la bonne exécution des processus de supervision et de gestion des évènements de sécurité et assure un reporting complet et précis des indicateurs clés. Il définit et pilote le plan d'amélioration des services du SOC.
Opérateur analyste SOC	L'opérateur analyste SOC assure la supervision du système d'information de l'organisation afin de détecter des activités suspectes ou malveillantes. Il identifie, catégorise, analyse et qualifie les évènements de sécurité en temps réel ou de manière asynchrone sur la base de rapports d'analyse sur les menaces. Il contribue au traitement des incidents de sécurité avérés en support des équipes de réponse aux incidents de sécurité.
Responsable du CSIRT	Le responsable du CSIRT (Computer Security Incident Response Team) ou du CERT (Computer Emergency Response Team) est responsable d'une équipe de réponse aux incidents de sécurité ciblant les systèmes d'information de l'organisation. Il s'assure de la bonne exécution des investigations et de la coordination des parties prenantes lors d'un incident de sécurité. Il contribue à la préparation de l'organisation pour garantir une réponse efficace. Lors d'incidents à fort impact, le responsable du CSIRT est amené à interagir avec l'équipe de gestion de crise.
Analyste réponse aux incidents de sécurité	L'analyste réponse aux incidents de sécurité intervient généralement au sein d'un CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team). En cas de soupçons sur une activité malveillante ou d'attaque au sein du système d'information, l'analyste réponse aux incidents de sécurité analyse les symptômes et réalise les analyses techniques sur le système d'information. Il identifie le mode opératoire de l'attaquant et qualifie l'étendue de la compromission. Il fournit des recommandations de remédiation pour assurer l'assainissement et le durcissement des systèmes attaqués.
Gestionnaire de crise de cybersécurité	Le gestionnaire de crise de cybersécurité intervient souvent au sein d'un CSIRT (Computer Security Incident Response Team) ou d'un CERT (Computer Emergency Response Team) externe ou interne pour grandes organisations, ou bien dans une équipe dédiée à la gestion de crise travaillant étroitement avec le CSIRT. Il analyse l'ampleur de la crise, met en place les actions nécessaires à sa résolution et coordonne les équipes pour qu'elles appliquent ses recommandations. Il conseille les directions métiers afin de résoudre les crises de cybersécurité. Il organise la capacité de l'organisation à affronter de nouvelles menaces en matière de cybersécurité.
Analyste de la menace cybersécurité	L'analyste de la menace cybersécurité étudie l'évolution des motivations et des modes opératoires des attaquants afin de permettre à l'organisation d'ajuster sa stratégie de cybersécurité. À un niveau plus opérationnel et technique, il fournit aux CERT/ CSIRT et aux SOC des renseignements fiables et contextualisés leur permettant d'adapter et d'améliorer leurs moyens de prévention, de détection et de réponse à incident.

MEMBRES DU GROUPE DE TRAVAIL RPS

Sébastien MERIOT — Head of CSIRT - OVH

Ma passion pour la cybersécurité est née le jour où mon PC a été frappé par le virus WIN32/CIH. Ce premier "incident" fut une révélation et m'a conduit vers ce qui allait devenir ma vocation. Depuis 2018, je dirige un CERT, où je mets mon expertise et mon enthousiasme au service de la protection des systèmes et des données. Toujours animé par la même curiosité et la même énergie qu'à mes débuts, je continue à faire de la sécurité informatique bien plus qu'un métier : une véritable mission.

Olivier RUET-CROS — CERT-Santé - FSSI Adjoint au Ministère des Affaires Sociales

Fort d'un parcours de 7 années dans l'enseignement et la recherche, suivi de 4 années en tant qu'analyste forensique au sein d'un CERT, j'occupe aujourd'hui le poste de FSSI adjoint auprès des Ministères Sociaux. Curieux et polyvalent, je suis animé par une passion profonde pour les enjeux de la cybersécurité. Mon engagement se traduit par une implication constante, qu'il s'agisse de problématiques stratégiques, opérationnelles, techniques ou humaines.

Anthony CHARREAU — CERT Crédit Mutuel Euro-Information

Après des études d'ingénieur en informatique et 8 années passées dans une ESN spécialisée en réseaux et télécom en tant que Directeur Technique et Directeur Adjoint des Opérations, j'ai rejoint Euro-Information, la filiale informatique interne de Crédit Mutuel Alliance Fédérale, il y a 11 ans : d'abord en charge des infrastructures réseaux puis depuis 6 ans dans la sécurité informatique. J'encadre actuellement les équipes opérationnelles internes de cyberdéfense (CERT, SOC et VOC), sous la responsabilité directe du Président de l'Entreprise.

Benjamin BILLON — CERT-FR - Responsable des partenariats opérationnels secteur privé

Aujourd'hui responsable des partenariats opérationnels avec le secteur privé au sein du CERT-FR, la sous-direction Opérations de l'ANSSI, j'ai précédemment passé une vingtaine d'années au sein d'un «Abuse Desk», littéralement «bureau des plaintes». Cette expérience, ainsi que mon implication dans l'écosystème, m'ont permis de prendre la mesure de la prévalence des risques psychosociaux particuliers liés à ces métiers.

David QUESADA — CSIRT-PWC - Directeur Cyber

Actuellement, directeur Cyber au sein de PwC France et Maghreb, j'ai exercé au sein du CERT du ministère des Armées ainsi qu'au CERT aDvens pendant en tout plus de 10 ans. Les gestions de crise et réponse à incident m'ont fait prendre conscience de l'importance de l'humain dans les métiers des CERT et notre manque de préparation tant comme collaborateur que responsable.

Les membres du GT RPS remercient Samuel De Cruz, du CERT aDvens pour sa relecture et son expertise en psychologie.

En 2024, l'association a lancé la première étude nationale sur les risques psychosociaux (RPS) auprès des CERTs, initiative unique à ce jour en France. Cette enquête pionnière a été conduite auprès de la communauté complète de l'association, soit environ 1 000 membres, couvrant l'ensemble des profils : responsables de la sécurité, analystes SOC, administrateurs, managers, personnels de support et élus associatifs.

MÉTHODOLOGIE

La collecte des données s'est déroulée entre le début du mois de septembre et le 30 octobre 2024 via le logiciel d'enquêtes Le Sphinx.

Le questionnaire, élaboré par le Groupe de Travail RPS et validé selon le Règlement Intérieur de l'association, combinait :

- des données sociodémographiques (statut, fonction, ancienneté, secteur d'activité),
- des échelles standardisées sur les principaux facteurs de RPS (charge de travail, autonomie, soutien, reconnaissance, climat relationnel, harcèlement...),
- des questions ouvertes permettant aux répondants d'exprimer librement leurs perceptions et suggestions.

Périmètre de l'étude :

Population cible	L'ensemble des membres d'InterCERT France (~1 000 personnes).
Profils inclus	Salariés, postes techniques.
Modalité	Enquête exhaustive en population cible.

Accès aux données :

Seules les personnes salariées de l'association ont accès aux données brutes, analysées uniquement sous forme agrégée.

La participation était volontaire et anonyme, et conforme aux principes de confidentialité et de protection des données personnelles.

L'objectif de cette initiative est double :

- Mesurer la prévalence et l'intensité des risques psychosociaux au sein de la communauté des CERTs, en identifiant les profils les plus exposés,
- Produire des recommandations concrètes et opérationnelles, pour améliorer la qualité de vie au travail et la résilience individuelle et collective des professionnels de la cybersécurité.
- Cette première étude constitue une référence unique et la seule évaluation globale des RPS spécifiquement dédiée aux CERTs en France, offrant des enseignements précieux pour l'ensemble du secteur.

MODE DE RECUEIL ET PÉRIMÈTRE DE L'ÉTUDE

L'étude a été menée entre septembre et octobre 2024 via la plateforme Le Sphinx, sur la base d'un questionnaire structuré comprenant des données sociodémographiques, des échelles standardisées de mesure des risques psychosociaux (RPS), ainsi que des questions ouvertes. La participation était volontaire et anonyme, et les résultats ont été analysés uniquement sous forme agrégée.

Le panel obtenu est équilibré et représentatif du marché français de la cybersécurité. Il présente une répartition variée des profils métiers (analystes SOC, responsables CERT, gestionnaires de crise, etc.) et une diversité d'entités :

CERTs internes : 53 %

CERTs externes /commerciaux : 31.6 %

CERTs institutionnels : 15.4 %

La proportion de femmes dans l'échantillon est de 18 %, ce qui correspond aux chiffres observés dans les études européennes récentes :

Étude ISC2 Europe 2024 : 18 % de femmes dans la cybersécurité

Allemagne : 14.6 %

Royaume-Uni : 17.9 %

(Sources : Le Figaro, Observatoire ANSSI 2022)

Répartition par âge

La distribution des classes d'âge est relativement homogène, avec une forte concentration dans la tranche 30-45 ans, qui constitue le cœur opérationnel des CERTs :

Cette homogénéité est jugée positive, car elle permet une lecture cohérente des résultats tout en mettant en lumière les enjeux spécifiques à cette tranche d'âge, notamment en matière de surcharge et de résilience.

Expérience professionnelle

Les répondants sont majoritairement expérimentés :

Cela témoigne d'une certaine maturité du secteur et d'une stabilité des parcours professionnels.

Taille des équipes

Les équipes CERT/CSIRT/SOC sont principalement de taille moyenne :

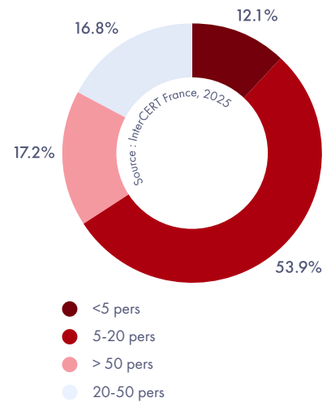
Ce découpage reflète une organisation agile mais suffisamment structurée pour répondre aux enjeux cyber.

Rôles au sein des équipes

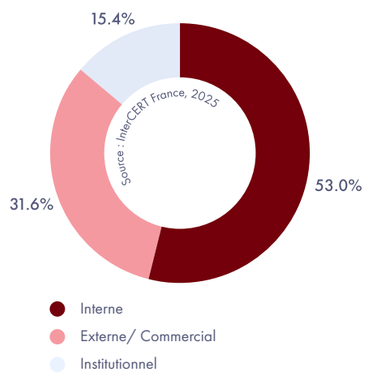
Les fonctions représentées sont diverses :

Cette diversité permet une lecture fine des résultats, en tenant compte des spécificités liées aux fonctions exercées.

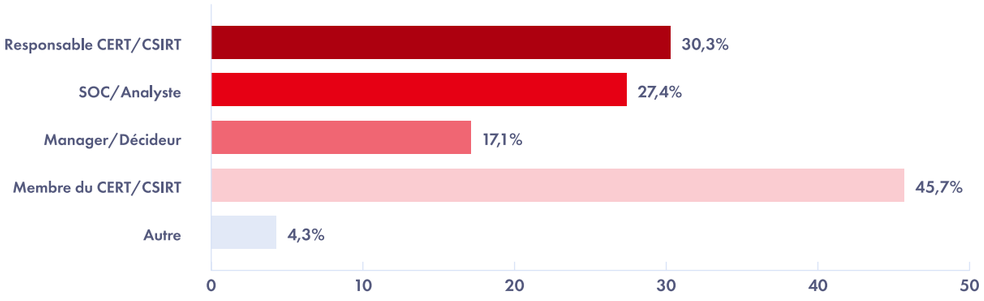
Quelle est la taille de votre équipe CERT/CSIRT/SOC ?



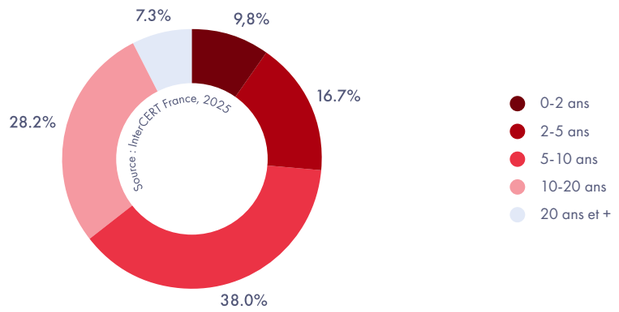
Quel «type» de CERT/CSIRT/SOC ?



Rôle au sein de l'équipe :

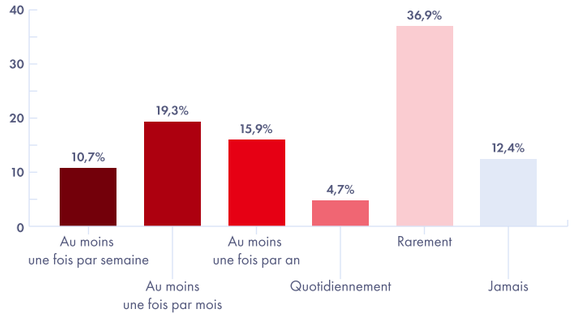


Depuis combien de temps exercez-vous votre métier cyber (pas uniquement dans votre entreprise actuelle) ?



PRÉSENTATION DES RÉSULTATS

A quelle fréquence estimez-vous être confronté à des problématiques éthiques au sein de votre travail ? (par exemple : la surveillance des collaborateurs)



Qu'est-ce que l'on entend par problématiques éthiques ?

Les problématiques éthiques en cybersécurité sont multiples. Est mentionné par exemple la prévention de la malveillance interne qui peut parfois basculer dans la surveillance de collaborateurs avec une véritable question sur l'équilibre entre la sécurité de l'entreprise et le respect des droits individuels des salariés. Un autre cas de figure se posant régulièrement est celui de la veille en menaces où la collecte de données permettant d'identifier des fraudeurs ou des attaquants. En effet, le RGPD prévoit que cette collecte est autorisée dans le cas où ces données permettent de protéger l'entreprise, mais la ligne reste très fine.

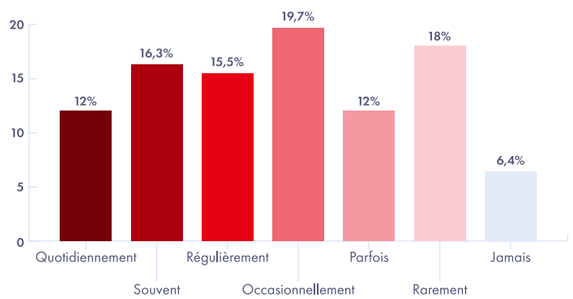
Le fait de constamment devoir apprécier ce qui est acceptable ou non est une véritable charge mentale pour les équipes.

Notre métier est la protection des intérêts de l'entreprise

(la surveillance des collaborateurs, équilibre de l'entreprise et respect individuel, collecte des données personnelles)

Sur les problématiques éthiques, il y a 30% des répondants qui sont confrontés une fois par mois et 49% qui le sont rarement ou jamais.

Etes-vous souvent amené(e) à traiter des contenus de nature illicite ou sensible dans le cadre de vos missions ? Données confidentielles ou sensibles, informations d'enquête, informations de nature criminelle, ...



Points clés :

- 43.8 % des répondants déclarent être exposés fréquemment à des contenus sensibles (quotidiennement, souvent ou régulièrement).
- 31.7 % y sont exposés de manière ponctuelle (occasionnellement ou parfois).
- 24.4 % y sont rarement ou jamais confrontés.

Interprétation :

- L'exposition à des contenus sensibles est courante dans les métiers du CERT/CSIRT/SOC, ce qui peut avoir des implications en matière de charge mentale, de résilience psychologique, et de besoin de soutien organisationnel.
- Le fait que près de 1 professionnel sur 2 soit régulièrement confronté à ce type de contenu souligne l'importance de protocoles de gestion émotionnelle, de formation à la gestion de l'information sensible, et éventuellement de dispositifs de soutien psychologique.
- À l'inverse, une part non négligeable (près d'un quart) n'est que rarement ou jamais exposée, ce qui peut refléter des différences de rôles ou de périmètres d'intervention au sein des équipes.

1/8 est confronté à du contenu de nature illicite ou sensible et 43,8% sont exposés au moins régulièrement à ce type d'information.

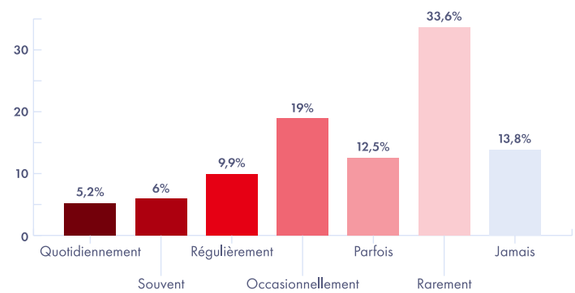
C'est plus de 60% au moins occasionnellement, soit plus d'6 répondant sur 10.

Ce qui est entendu par contenu illicite ou sensible : des données confidentielles ou sensibles, des informations d'enquêtes, des éléments criminels, terroristes.

En revanche quand il s'agit de donnée psychologiquement difficiles 5,2% sont confrontés quotidiennement et plus d'1 répondant sur 5 régulièrement (21,1%).

C'est plus d'4 répondants sur 10 au moins occasionnellement.

Etes-vous souvent exposé à des contenus psychologiquement difficiles ? (Contenu licites ou choquants, criminels, informations personnelles sur autrui, ...



Points clés :

- 31.1 % des répondants sont exposés fréquemment ou ponctuellement à des contenus psychologiquement difficiles (quotidiennement, souvent, régulièrement/occasionnellement).
- 46.1 % y sont exposés rarement ou jamais, ce qui représente une majorité relative.
- 12.5 % déclarent y être exposés parfois, ce qui reflète une exposition intermédiaire

L'exposition à des contenus psychologiquement difficiles est moins fréquente que celle aux contenus sensibles ou confidentiels (cf. tableau 2.1.3), mais reste significative pour près d'un tiers des professionnels.

Cela peut avoir des impacts émotionnels et cognitifs, notamment pour ceux qui y sont confrontés régulièrement, et souligne l'importance de :

- Dispositifs de soutien psychologique
- Formations à la gestion du stress et des émotions
- Encadrement éthique et déontologique dans le traitement de ces contenus

Le fait que près de la moitié des répondants soient rarement ou jamais exposés peut refléter une répartition fonctionnelle des rôles, où certains métiers sont plus exposés que d'autres (ex. : analystes SOC vs gestionnaires de crise).

Les données manipulées par les équipes sont pour la plupart des données sensibles ou critiques pour leur entité ou les entreprises qu'ils soutiennent. La nature des recherches en anticipation, de la détection de comportement malveillant, l'analyse forensique ainsi que les gestions de crise oblige à l'accès régulier à ce type d'information avec des contenus choquants.

Il est important que chacun puisse se rendre compte de la fréquence et du stress engendré.

Avez-vous suffisamment de temps pour accomplir vos missions ?

57.3 % estiment avoir globalement assez de temps, mais 42.7 % jugent ne pas en avoir suffisamment, ce qui révèle une pression temporelle significative pour près de la moitié des répondants.

La charge d'incidents vous semble-t-elle raisonnable ?

70.4 % considèrent que la charge d'incidents est globalement raisonnable, ce qui est plutôt positif, même si près d'un tiers la jugent excessive.

Disposez-vous de suffisamment de ressources pour accomplir vos missions ?

62.4 % estiment avoir des ressources suffisantes, mais plus d'un tiers (37.6 %) jugent leurs moyens insuffisants, ce qui peut impacter la qualité du travail et la santé mentale.

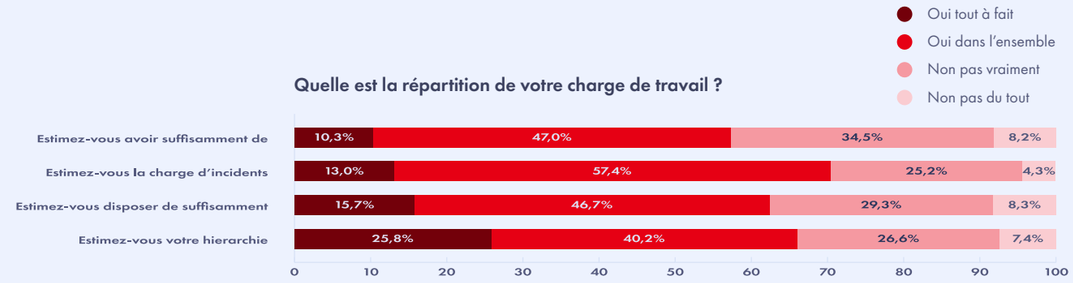
Votre hiérarchie est-elle consciente de votre charge de travail ?

66 % pensent que leur hiérarchie est globalement consciente de leur charge, mais 34 % expriment un manque de reconnaissance ou de compréhension, ce qui peut générer du désengagement ou du stress organisationnel.

CONCLUSION

La majorité des répondants ont une perception plutôt positive de leur charge de travail et des ressources disponibles.

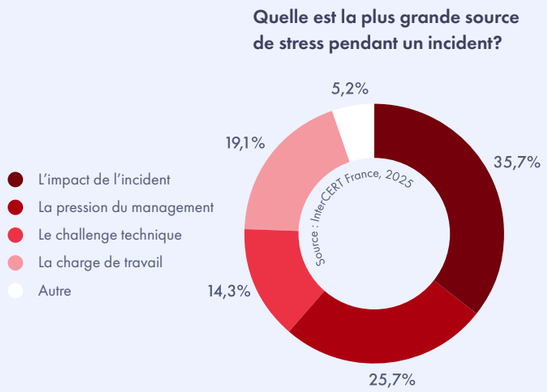
Toutefois, une partie significative (30 à 40 %) exprime des difficultés liées au temps, aux moyens ou à la reconnaissance, ce qui mérite une attention particulière dans les politiques RH et managériales.

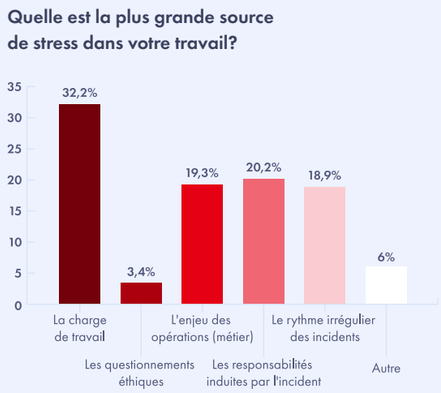


La charge de travail domine largement, ce qui pourrait indiquer un besoin de rééquilibrage des tâches, de renforts humains ou de meilleure priorisation.

Les incidents (responsabilités et rythme) représentent ensemble près de 39%, ce qui souligne leur impact sur le stress.

Les questionnements éthiques, bien que minoritaires, pourraient nécessiter une attention particulière en termes de formation ou de soutien moral.





Le stress lié à l'impact est le plus fort, ce qui souligne l'importance de la gravité perçue des incidents.

La pression du management est aussi un facteur clé, ce qui pourrait appeler à des pratiques de communication plus sereines ou à une meilleure coordination pendant les crises.

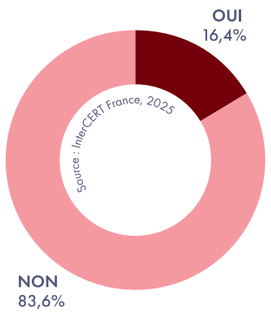
Le challenge technique est moins stressant que les facteurs humains ou organisationnels, ce qui peut indiquer une bonne maîtrise technique mais un besoin de soutien sur les aspects relationnels ou décisionnels.

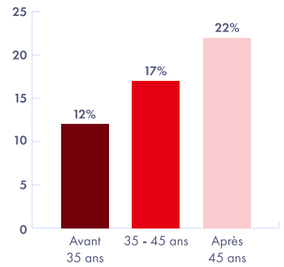
FACTEURS DE STRESS

GESTION DU STRESS

1 répondant sur 6 se dit préparé et une progression avec l'âge est observé

Estimez-vous avoir été préparé à la gestion du stress inhérent à un CERT/CSIRT/SOC?



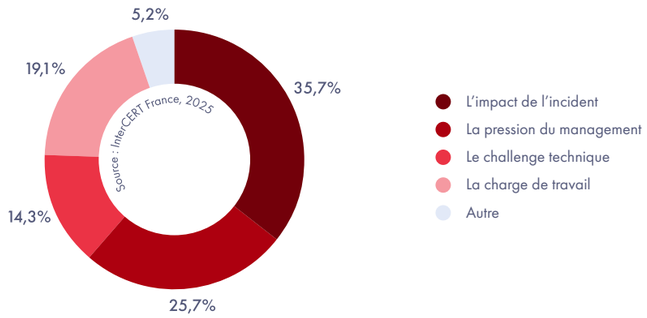


Cela peut traduire :

- Un apprentissage qui se fait davantage par l'expérience et les situations professionnelles vécues que par la formation initiale ou par une formation professionnelle dispensée dès le début de carrière
- Une maturité / capacité à davantage relativiser les choses et être moins affecté personnellement par un évènement vécu avec l'âge qui avance

Il est communément admis que le métier de la réponse sur incidents, ou plus largement les métiers de la cybersécurité, sont exposés à des situations pouvant provoquer du stress, occasionnellement ou plus fréquemment.

Quelle est la plus grande source de stress pendant un incident?



TLP:CLEAR

SOURCES DE STRESS

Du constat, il serait par exemple intéressant de mettre en œuvre des initiatives concrètes (connaissance de soi et de son fonctionnement propre en conditions normales, de stress ou de fort stress) pour prendre conscience de son état, puis l'apprentissage de leviers actionnables concrètement pour traiter et gérer la situation au mieux.

Il pourrait être pertinent également que les organisations prennent conscience du besoin de dispenser des formations d'expertise technique mais également des formations de développement personnel, qui contribuent activement à permettre aux collaborateurs d'être plus compétents et mieux armés pour gérer les situations opérationnelles auxquelles ils sont confrontés, y compris dans leur volet non technique.

Les techniques de gestion du stress peuvent s'apprendre avec le temps avec une certaine forme de prise de recul, mais il est important de se former régulièrement. Les manager et pilotes devraient pouvoir accéder à des formations de gestion de son stress mais aussi du stress des autres pour « être un absorbeur de stress et un diffuseur de sérénité ».

Proposition 2 :

Sur la base de ce constat, la mise en place d'initiatives concrètes visant à améliorer la connaissance de soi, notamment en conditions normales, sous stress ou en situation de stress intense, apparaît pertinente. Ces actions permettent aux individus de prendre conscience de leur état et favorisent l'acquisition de leviers opérationnels pour gérer efficacement diverses situations.

Au global, 1 répondant sur 2 a eu des collègues en arrêt de travail

Il serait également opportun que les organisations reconnaissent l'importance d'organiser non seulement des formations techniques spécialisées, mais aussi des sessions dédiées à la gestion du stress. Ce double volet contribue activement à renforcer les compétences des collaborateurs, leur permettant de mieux appréhender l'ensemble des enjeux rencontrés sur le terrain, y compris ceux relevant du domaine non technique.

Ces techniques requièrent un apprentissage progressif et une capacité de recul. Il demeure essentiel de promouvoir une formation continue afin d'améliorer ces compétences. Il est recommandé que les managers et pilotes aient accès à des programmes formatifs axés tant sur la gestion de leur propre stress que sur celle de leurs équipes, afin de favoriser un climat de sérénité et d'efficacité au sein de l'organisation. « Être absorbeur de stress et diffuseur de sérénité ».

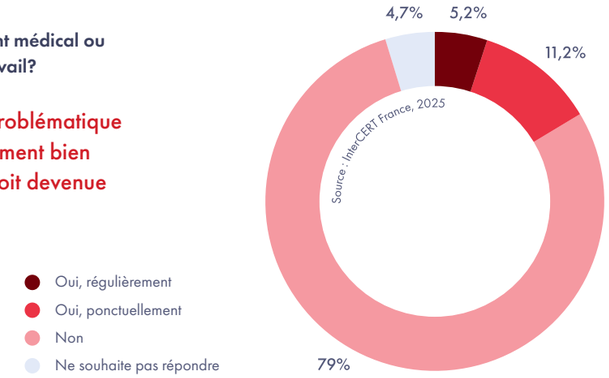
Plus de 16% ont reçu un accompagnement médical ou psychologique en lien avec les conséquences de leur travail

Bonne préparation, prise de conscience et mise à disposition de leviers devrait permettre de réduire l'impact personnel pour les collaborateurs exposés, permettant notamment d'aboutir à une réduction des débordements induits et notamment des arrêts de travail.

TLP:CLEAR

Avez-vous déjà fait l'objet d'un accompagnement médical ou thérapeutique lié aux conséquences de votre travail?

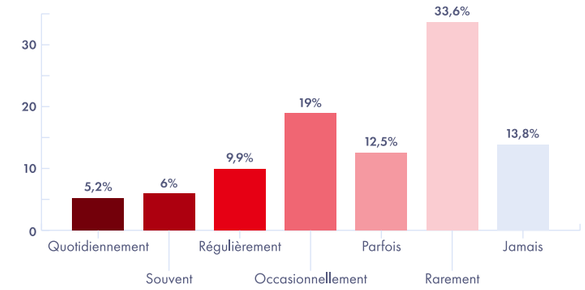
Cela démontre l'existence concrète de la problématique et laisse craindre un besoin d'accompagnement bien supérieur avant que la situation vécue ne soit devenue problématique.



CONTENUS PSYCHOLOGIQUEMENT DIFFICILES

Etes-vous souvent exposé à des contenus psychologiquement difficiles ? (Contenus illicites ou choquants, criminels, informations personnelles sur autrui, ...)

86% des répondants sont exposés, plus ou moins fréquemment, à des contenus psychologiquement difficiles.



Il s'agit d'une autre spécificité de notre métier : les analystes sont potentiellement exposés, plus ou moins fréquemment, à une variété de contenus pouvant choquer. Ils enquêtent potentiellement sur des individus pratiquant des actes illicites et condamnables. Même s'ils n'en ont pas forcément conscience de manière immédiate, ce qui a été vu peut continuer de ronger les analystes longtemps encore après leur exposition.

Il est important de prendre conscience de la problématique et du risque, de sensibiliser et de former les collaborateurs exposés et de leur permettre de verbaliser ces situations dans un dispositif adapté et préservant la confidentialité des propos relatés.

L'exposition aux contenus sensibles ou choquants constitue un facteur de risque psychosocial important pour les équipes CERT et SOC.

Selon l'étude InterCERT France 1 répondant sur 5 déclare être quotidiennement, souvent ou régulièrement confronté à ce type de contenus. Lorsqu'il s'agit de données psychologiquement difficiles, 5,2% y sont exposés chaque jour, et 21,1% de manière régulière. Au total, plus de 4 répondants sur 10 y sont confrontés au moins occasionnellement.

Les données manipulées par ces équipes sont majoritairement sensibles ou critiques, tant pour leur propre entité que pour les organisations qu'elles soutiennent. Les activités telles que la recherche en anticipation, la détection de comportements malveillants, l'analyse forensique ou la gestion de crise impliquent un accès fréquent à des informations potentiellement choquantes ou émotionnellement lourdes.

Il est essentiel de mettre en place un suivi spécifique pour les collaborateurs régulièrement exposés à ces contenus, qu'il soit institutionnel (via la médecine du travail), commercial (via des prestataires spécialisés) ou interne (via des dispositifs RH ou psychologiques dédiés).

Ce suivi doit permettre à chacun de prendre conscience de la fréquence de cette exposition et de mieux réguler le stress qu'elle peut engendrer.

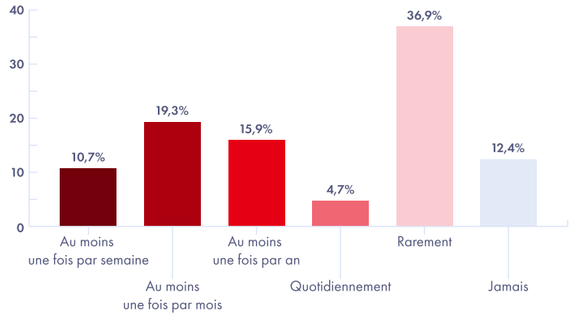
Plan d'actions face au stress

1. **Prévention et sensibilisation**
   - ► Campagnes internes sur les effets du stress et les bénéfices du soutien psychologique.
   - ► Formations pour les managers sur la détection des signaux faibles et l'orientation vers les bons dispositifs.
2. **Renforcement des dispositifs d'accompagnement**
   - ► Mise en place ou amélioration d'un programme de soutien psychologique (ex. : ligne d'écoute, psychologue du travail).
   - ► Accès facilité à des consultations ponctuelles (sans prescription, anonymes si possible).
3. **Culture d'entreprise bienveillante**
   - ► Encourager une parole libre sur la santé mentale sans stigmatisation.
   - ► Intégrer des rituels de décompression (groupes de parole, ateliers bien-être, etc.).
4. **Suivi et évaluation**
   - ► Réaliser des enquêtes régulières pour suivre l'évolution du recours aux soins.
   - ► Mettre en place des indicateurs de bien-être dans les tableaux de bord RH.
5. **Communication ciblée**
   - ► Adapter les messages selon les profils : certains peuvent être plus réceptifs à des témoignages, d'autres à des chiffres ou à des garanties de confidentialité.

PROBLÉMATIQUES ÉTHIQUES

1 répondant sur 2 est exposés davantage que « rarement » ou « jamais » à des problématiques éthiques

A quelle fréquence estimez-vous être confronté à des problématiques éthiques au sein de votre travail ? (par exemple : la surveillance des collaborateurs)



Les actions menées par les équipes de réponse sur incident doivent impérativement s'inscrire dans un cadre formel et structuré, garantissant la légitimité des interventions réalisées. Cette exigence est directement liée à la nature potentiellement intrusive des investigations, qui peuvent concerner la confidentialité des activités professionnelles, voire personnelles, des collaborateurs.

En l'absence de cadre clair, les analystes peuvent être amenés à s'interroger sur le bien-fondé des demandes qui leur sont adressées, notamment sur le plan éthique. Cette situation les place dans une position délicate, où le refus d'exécuter une injonction jugée douteuse pourrait leur être préjudiciable.

La mise en place de processus internes clairs et de dispositifs de sensibilisation permettrait aux équipes de mieux appréhender ces situations, de connaître les procédures de déclaration et de suivi, et d'identifier les moyens de mise en sécurité du collaborateur concerné.

Par ailleurs, la détection et la catégorisation de contenus sensibles nécessitent des formations régulières sur les cadres législatifs applicables dans les pays d'intervention. Pour les équipes susceptibles d'agir à l'international, il est essentiel de disposer d'un processus accessible et connu permettant d'obtenir rapidement des informations fiables sur les obligations légales en matière de réponse à incident ou de recherche OSINT.

TLP:CLEAR

SUR-SOLLICITATIONS EN PÉRIODE D'INCIDENT

1 répondant sur 2 est concerné

Seuls les équipes de plus de 50 collaborateurs sont davantage épargnées avec 35% des répondants concernés

Un incident cyber est un évènement stressant par nature, avec un fort enjeu potentiel pour la victime pouvant aller jusqu'à la survie même de l'entité.

Cela peut se traduire par des sollicitations des équipes intervenant sur l'incident venant de multiples horizons et en direct : direction générale, décideurs informatiques, équipes métiers qui ne peuvent plus travailler normalement, simples collaborateurs, clients, partenaires, fournisseurs, journalistes, etc.

Il est important de prendre conscience de cette problématique et d'organiser les interactions possibles ou non avec l'équipe de réponse sur incidents, seule à même de traiter l'incident lui-même et progresser dans sa compréhension ainsi que sa résolution. En l'absence d'une bulle de protection suffisamment présente, l'équipe de réponse sur incident va être perturbée par ces sollicitations, perdre de la concentration voir perdre du temps si elle doit réellement les traiter et apporter une réponse.

Une organisation de crise doit être prévue et les interactions possibles en contexte de crise doivent être documentées à l'avance. Cela permet à l'équipe de réponse sur incidents de s'organiser pour traiter les sollicitations prévues, et de ne pas donner suite aux sollicitations non souhaitables en rappelant le cadre de gestion prévu.

Au-delà de la théorie, les exercices de crise permettent par ailleurs de mettre l'organisation en situation et s'assurer qu'elle est pertinente et satisfaisante, et aussi aussi d'instaurer des réflexes et automatismes avant d'avoir à traiter un cas réel.

L'importance de la formation des managers et pilotes

Ce constat est en lien avec la formation des managers d'équipes CSIRT / SOC. Dans les petites équipes, la gestion du temps et la mise en place des processus d'escalade n'est pas forcément le point le mieux géré. Les managers et les pilotes doivent être conscients de ces éléments. Leur action est d'être une sorte de « tampon » entre les demandes, pouvant être pressantes de clients ou de la hiérarchie si les temps de repos ne sont pas respectés ou pour éviter la sursollicitassions des équipes déjà sur des incidents. Quand le filtrage est insuffisant, les personnes peuvent en souffrir particulièrement, sans même que les responsables ou les pilotes ne le détectent.

TLP:CLEAR

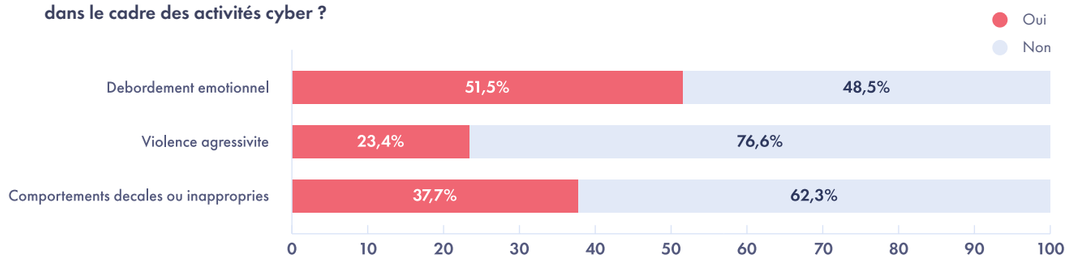
DISPOSITIFS DE CRISE

1 répondant sur 2 a constaté du débordement émotionnel

1 répondant sur 3 a constaté des comportements inappropriés

1 répondant sur 4 a constaté de la violence

Avez-vous déjà vu des collègues «craquer» au travail dans le cadre des activités cyber ?



Face aux conséquences potentiellement extrêmes induites par les incidents de sécurité informatique, les collaborateurs traitant l'incident ou intervenant auprès de leur client victime d'un tel incident peuvent être la cible ou assister à du débordement émotionnel, des comportements inadaptés voir de la violence verbale et/ou physique.

Ces comportements sont anormaux et n'ont pas leur place dans une cellule de crise ou une prestation réalisée. Cela doit être clairement encadré par le contrat de prestation ou les règles de fonctionnement de la cellule de crise, permettant le recadrage systématique de ces agissements. Il ne faut pas les laisser s'établir comme quelque chose de normal et accepté.

Même si la situation est extrême, elle se produit dans un contexte professionnel qui appelle à une nécessaire retenue.

Former l'ensemble du personnel et les responsables

Ce constat est en lien avec la formation à la gestion du stress pour toutes personnes qui peuvent être intégrées dans une crise ou une réponse à incident. Les exercices au plus proche d'une réalité permettent un apprentissage de tous. Il est important que les personnes de cellule de crise, de réponse à incident se connaissent au maximum pour appréhender les réactions qu'elles pourraient avoir. Il ne faut pas oublier qu'un jour le « vase puisse déborder » et qu'une personne stable et fiable ait une réaction inappropriée, la formation personnelle et collective doit permettre la meilleure gestion de cette situation ou de ces situations.

IMPLICATION DE RESSOURCES PERSONNELLES

43% des répondants utilisent des ressources personnelles pour réaliser leurs missions

C'est même jusqu'à 50% des répondants dans les équipes de 5 à 20 collaborateurs ainsi que dans les CERT externes et institutionnels

Les activités de réponse sur incident peuvent nécessiter un environnement technique spécifique : indépendance du système d'information à défendre, système d'exploitation et logiciels spécifiques, connexion à Internet indépendante de la connexion d'entreprise ou entité, mécanismes d'anonymisation, ...

Il est important que l'entreprise ou entité prenne en compte les besoins structurels des équipes de réponse sur incident, y compris s'ils sont atypiques par rapport au reste du système d'information, mais tout en restant adaptés et justifiés par rapport à la mission à réaliser, et dans un cadre d'usage documenté.

Il est préoccupant de constater la proportion de professionnels impliquant leurs ressources informatiques personnelles dans la réalisation de leur mission professionnelle, notamment compte tenu des données qui sont potentiellement manipulées dans le cadre des missions :

- Accès à des sites Internet malveillants, compromis, interdits
- Visualisation de contenus choquants, répréhensibles
- Manipulation de données confidentielles du client / de l'entreprise ou entité (RGPD)

La manipulation de ces contenus sur un dispositif informatique personnel, non remis par l'employeur, peut engager la responsabilité personnelle du collaborateur. Cela ne devrait jamais être fait en première intention ou par simple choix personnel, et dénote un potentiel écart entre les outils fournis par l'Entreprise et les besoins du collaborateur pour mener à bien ses missions.

TODO : Mise en danger des personnels et des familles de tomber sur des personnes Cyber qui ne font pas que du Cyber (Mafia, Militaires ...)

TODO : Warning, ce point et un point important qui n'a pas été traité dans le livre blanc. Elle pose néanmoins un risque important pour les collaborateurs / entreprises...

L'utilisation de moyen professionnel permet de protéger les collaborateurs des équipes car les menaces auxquelles elles peuvent être confrontées sont de différents types : militaires, mafias, cartels, hacktivistes violents pour les plus risqués. Il a été observé des acteurs malveillants qui appelaient directement les conjoins des administrateurs et / ou des RSSI pour leur mettre la pression. Ce point n'est pas traité dans ce livre blanc mais remonte un risque important pour les collaborateurs en plus des entités.

CADRE CONTRACTUEL

HORAIRES DE TRAVAIL

65% des répondants sont concernés par les sollicitations en dehors des horaires de travail

Les équipes de moins de 20 collaborateurs sont davantage concernées

Les CERT externes et institutionnels sont davantage concernés aussi (70% des répondants)

1 répondant sur 2 possède un cadre pour les sollicitations et déplacement en dehors des horaires habituels de travail

Le système d'information d'une entreprise ou entité reste généralement actif 24h / 24 et 7 jours sur 7, y compris dans son exposition externe (message email, sites internet, interconnexions avec des tiers, etc.)

Dans ce contexte, une attaque informatique peut intervenir à n'importe quel moment, y compris en dehors des horaires habituels de travail. Pour certaines typologies d'attaques, cela est même un choix délibéré de l'attaquant afin de maximiser le temps durant lequel il pourra agir sans être détecté, par exemple du vendredi soir au lundi matin en France.

Pour les équipes de réponse sur incident internes, ou pour les prestataires de réponse sur incident externes, il s'agit d'un point structurel à prendre en compte dans le fonctionnement de l'activité et des collaborateurs : des interventions en dehors des horaires habituels de travail de l'entreprise ou entité peuvent se produire.

Cela veut dire que le cadre de travail contractuel doit prévoir cette possibilité par anticipation, tout en respectant le code du travail Français (durée maximale de travail quotidien et hebdomadaire, temps de repos quotidiens et hebdomadaires, valorisation des heures supplémentaires, etc.)

Cela veut également dire que des accords peuvent être nécessaires et négociés par anticipation (accord d'astreinte, accord d'intervention hors heures ouvrées, ...)

Suivre les temps, c'est reconnaître l'investissement.

Les entités des collaborateurs doivent prendre en compte les contraintes horaires d'un travail en entraves non ouvrées. Une convention d'astreinte et de travail en heure non-ouvrée doit être en place ainsi qu'un suivi strict des heures des collaborateurs avec des moyens pour aider les managers et pilotes à gérer les plannings (eux aussi impactés par ces temps). Les contrats des collaborateurs doivent être clairs et explicités par les RH sur le traitement de ces temps. Les membres des équipes doivent avoir une attention toute particulière sur ce point lors de leur embauche, tant au niveau du contrat que de la convention collective ou convention d'entreprise.

PRISE EN COMPTE DES RISQUES PSYCHO SOCIAUX DANS L'ENTREPRISE

80% des répondants indiquent que l'entreprise ou entité prend en compte les RPS

72% considèrent les moyens mis en œuvre insuffisants

56% indiquent que le service RH pilote le sujet mais avec une approche générique ne répondant pas aux spécificités des métiers exercés

Les managers de proximité ont un rôle prépondérant pour sensibiliser les parties prenantes de l'entreprise ou entité (ligne hiérarchique, décideurs, RH) aux particularités du métier de réponse sur incident et veiller à ce qu'elles s'inscrivent dans un cadre plus systématique et générique, tout en approfondissant certains aspects plus spécifiques.

La bonne formation et préparation à la gestion de situations stressantes par exemple peut être une action générique pour partie (tests de personnalité pour se connaitre soi-même et savoir comment nous réagissons sous stress plus ou moins fort, boite à outils d'actions pour réguler l'impact d'une situation sur soi, ...) et complété par une action spécifique au métier exercé (application à une cellule de gestion de crise, exposition à des contenus choquants, action dans un contexte d'incertitude et à fort enjeu, ...)

Plan d'action RPS

1. **Renforcer la gouvernance RPS**

- Créer un comité RPS pluridisciplinaire (RH, managers, représentants métiers, médecine du travail).
- Nommer des référents RPS dans les équipes opérationnelles, formés aux signaux faibles et relais des dispositifs.

2. **Adapter les dispositifs aux spécificités métiers**

- Réaliser une cartographie des risques psychosociaux par métier, notamment pour les métiers de la réponse sur incident.
- Développer des protocoles spécifiques pour les métiers exposés à des contenus choquants, à l'urgence ou à l'incertitude.

3. **Former et outiller les collaborateurs**

- Formation générique :
  - Tests de personnalité pour mieux se connaître.
  - Outils de régulation du stress (respiration, ancrage, gestion émotionnelle).
  - Sensibilisation aux mécanismes du stress et du burn-out.
- Formation spécifique :
  - Simulations de gestion de crise.
  - Préparation à l'exposition à des contenus sensibles.
  - Techniques de prise de décision en contexte incertain.

4. **Soutien psychologique structuré**

- Mise en place d'un dispositif d'écoute psychologique accessible, confidentiel et réactif.
- Consultations ponctuelles ou régulières avec des psychologues du travail ou thérapeutes spécialisés.
- Débriefings post-incident systématiques pour les équipes exposées.

5. **Valoriser le rôle des managers de proximité**

- Former les managers à :
  - Identifier les signaux de détresse.
  - Adapter leur posture managériale selon les profils.
  - Être des relais actifs des dispositifs RPS.
- Leur donner des outils concrets pour animer des temps de parole, réguler les tensions, et remonter les besoins.

6. **Suivi et amélioration continue**

- Mettre en place des indicateurs de suivi RPS (absentéisme, turnover, recours aux dispositifs).
- Réaliser des enquêtes régulières pour ajuster les actions.
- Intégrer les RPS dans les revues de performance et de qualité de vie au travail.

ASPECTS CONTRACTUELS

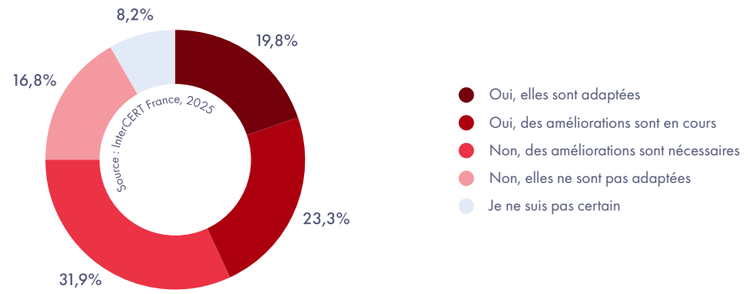
50% des répondants ne savent pas précisément ce que prévoit leur contrat de travail dans le cadre spécifique de leurs missions (les CERT externes et commerciaux sont les plus avertis)

57% ignorent si une protection juridique existe

20% seulement ont un cadre pour traiter des données illégales

La nature atypique des missions de réponse à incident nécessite un cadre contractuel spécifique lui aussi pour protéger les analystes et légitimer leurs actions.

Estimez-vous que les politiques et pratiques RH de votre entreprise sont adaptées aux besoins spécifiques de votre métier (gestion des incidents, rythmes de travail, etc)



Les contrats point de vigilence

Les collaborateurs gagneraient à être plus regardants et prudents sur les dispositions prévues par leur employeur dans la réalisation de leurs missions, afin que leur responsabilité personnelle ne soit pas d'être engagée en cas de difficultés ou d'enquêtes.

Les contrats des collaborateurs doivent être clairs et lisibles avec une explication par les RH régulière du traitement de ces temps. Les membres des équipes doivent avoir une attention toute particulière sur ce point lors de leur embauche, tant au niveau du contrat que de la convention collective ou convention d'entreprise.

LES MOTEURS DES RÉPONDANTS

Tout n'est pas si catastrophique, l'analyse met en avant des moteurs puissants au sein des CERTs tel que :

- Le Sens du travail pour 20%
- La diversité des missions pour 20%
- La cohésion d'équipes 15%
- Les défis techniques 15%
- Les autres sont la flexibilité, l'apprentissage permanent, la reconnaissance

Travailler dans un CERT ou SOC donne du sens à son travail car il permet d'anticiper, de détecter et de réagir face à des menaces pour le bien de la collectivité, des entreprises ou de son entreprise.

L'objectif principal est la protection.

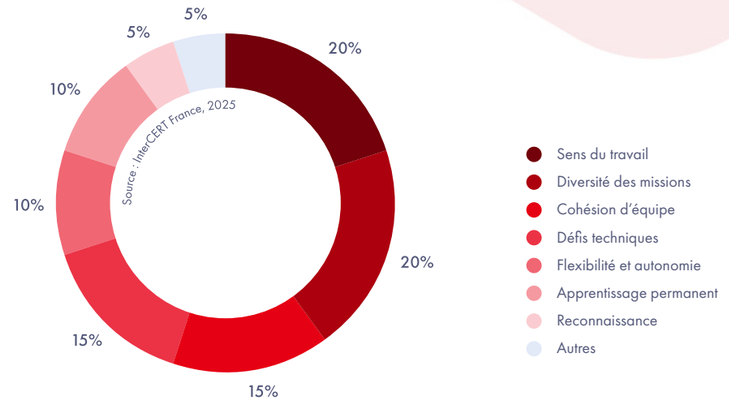
Les principales familles de facteurs de risque sont très liées aux moteurs des répondants :

- Exigence émotionnelle
- Exigence de travail
- Conflits de valeurs
- Insécurité de la situation au travail
- Rapports sociaux et relations au travail
- Autonomie et marges de manœuvre

Les éléments moteurs peuvent entraîner vers une dérive et une sensation de ne pas en faire suffisamment ou qu'il faudrait en faire plus. Cet élément moteur pousse parfois à oublier qu'il faut prendre soin de soi afin de prendre soin des autres. Sans cette réciprocité les risques de burn-out, épuisement, dérive liée au stress augmentent considérablement.

Les équipes le disent clairement le sens du travail et sa diversité en font une force. Leur engagement est une vraie chance pour l'ensemble de la communauté et l'écosystème.

N'est-il pas de notre responsabilité de maintenir ces forces dans un cadre émotionnel maitrisé ?



L'association est attendue par 90% des répondants pour proposer des solutions. L'association ne compte pas se dérober à la demande et propose des pistes de réflexion concrète.

PRÉCONISATIONS ET PISTES D'ACTION/PRISE EN CHARGE DES RPS PAR L'EMPLOYEUR

La prise en charge des RPS au sein d'une entreprise, d'une équipe ou d'un service peut être considérée selon deux approches différentes. Les préconisations et pistes de réflexion ci-dessous s'articulent autour de ces axes et proposent une répartition des mesures en fonction des différents services d'une structure (direction, RH, management, collaborateurs - collaboratrices, ...)

RÉACTION ET PRISE EN CHARGE INDIVIDUELLE

Dans un premier temps, la prise en charge des RPS peut être abordée comme un problème de santé au travail de collaborateurs précis. Autrement dit, considérer que les analystes, pilotes de CERT et SOC sont soumis aux RPS et qu'il faut les suivre et les accompagner individuellement.

Dans cette approche, décrite dans la présente section, l'idée est de mettre en avant tous les outils pour créer des environnements de travail adéquats pour que tout un chacun puisse travailler dans de bonnes conditions, qu'il s'agisse de mesures préventives ou réactives. Par exemple un accompagnement par la médecine du travail, la détection des signaux et alertes avant-coureurs, etc... La présente partie se veut la plus concrète possible, aussi les préconisations proposées sont séparées selon les strates concernées.

Pour les services de direction

- Porter la culture d'entreprise autour des RPS
- Se rapprocher et assurer la diffusion de programmes généraux ou nationaux sur le sujet des RPS et de la santé mentale en entreprise

Pour les services RH

- Rendre possible de partager (au sein de l'équipe, ou avec des tiers formés) autour des contenus potentiellement choquants rencontrés : dans quel cadre, de quelle nature, en quelle quantité, ...
- Définir et identifier des psychologues d'entreprise (internes ou bien liés à la médecine du travail par exemple).
- Former à l'appui et à l'écoute : bienveillance active, détection des signaux d'alerte, espaces "sûres", ...
- Définir des cadres d'échanges (formels ou informels) permettant de remonter et d'échanger sur les situations considérées comme humainement ou éthiquement difficiles.

Pour les managers

- Rendre possible de renvoyer le message "je suis en surcharge" sans risque de sanction ou de dévalorisation
- Encourager les pauses et microcoupures
- Adapter le rythme de travail global aux enjeux des incidents et des équipes CERT et SOC : souplesse des horaires hors incidents, modularité du rythme, ...
- Cadrer la culture d'équipe :
  - Rappeler que les arrêts maladie sont légitimes (pas une faveur), et que ce sont des signes de responsabilité
  - Montrer l'exemple : respecter ses propres temps de repos, valoriser la vigilance dans l'équipe, ...
  - Inclure la question de la santé et de l'état émotionnel dans les revues d'incidents, et les échanges d'équipe plus largement
  - Travailler le discours, éviter la culpabilisation
- Diffuser l'annuaire des contacts d'aide : référents, médecine du travail, cellule RH, ...

Pour les collaborateurs et collaboratrices

- Être formé à la connaissance de soi, les techniques de respiration, les approches pour se recentrer et détecter ses limites ...
- Être alerte aux signaux faibles : changement d'attitude ou d'humeur, isolement, changement brutal de rythme de travail, suraccumulation d'heures tardives, réactivité forte hors des heures de bureau, ...
- Créer des opportunités d'échange et de dialogue
- Se faire le vecteur de la culture d'équipe
- Lorsqu'il y a un mal-être, la situation est rarement seulement individuelle. Partager autour de soi permet de détecter les possibles autres collègues en difficulté.

RÉFLEXION ORGANISATIONNELLE

Par ailleurs, on peut considérer que les RPS et leurs conséquences les plus extrêmes (burn-outs, arrêts de travail prolongés, ...) sont les symptômes visibles d'un service dysfonctionnel, et doivent être adressés comme la partie émergée d'un iceberg.

Ainsi, une approche plus structurelle utilisant les RPS comme un moyen de réflexion sur les processus et dynamique d'équipe permettrait de mieux organiser le travail et limiterait l'émergence de ces symptômes.

Ainsi, les mesures de prévention tournent davantage autour de l'organisation et des mécaniques internes aux équipes. De manière générale :

Pour les services de direction

- Intégrer les enjeux règlementaires liés aux RPS (ex : ISO45003) dans les modèles de risques
- Assurer une formation ciblée et thématique des managers
- Définir des indicateurs permettant de remonter et observer les alertes
- Assurer que les cadres de travail à risques (astreintes, rotations, ...) sont organisés et pris en compte correctement

Pour les services RH

- Prévoir des cadres contractuels clairs sur le traitement des données illicites dans le cadre des incidents
- Définir des référents ou référentes RPS (sur le modèle du harcèlement)
- Prise en compte des enjeux de sécurité et d'incidents dans les modèles contractuels
- Prévoir ces mêmes enjeux dans le cadre des contrats avec des prestataires
- Prévoir un cadre contractuel sur l'instauration d'astreintes d'incidents
- Formations et préparation
  - Formation à la gestion du stress pour l'ensemble des équipes CERT et SOC
  - Formation des autres managers aux enjeux des rythmes CERT et SoC

Pour les managers

- Cadrer et répartir efficacement la charge
  - Mise en place d'astreintes
  - Equipes tournantes en 3x8
  - Débordement sur des prestataires ou équipes partenaires
  - Organiser des réunions de suivi
  - Prévoir des plages de repos systématiques entre les incidents
  - Donner des moyens aux collaborateurs et collaboratrices de signaler la surcharge de travail : il est très difficile d'estimer la charge d'un incident spécifique, aussi les outils de suivi classiques (orientés pour de la gestion de projet) ont bien souvent des angles morts sur ces éléments.
  - Définir un roulement structuré pour déterminer qui s'occupe de chaque incident entrant : cela permettra de lisser la charge (réelle et émotionnelle) mais aussi de ne pas laisser de personne de côté
- Créer des solutions permettant de remonter des problèmes et signaux d'alerte : canaux et messageries anonymes, face-à-face managériaux, prévoir des plages sur les sujets humains et santé dans les réunions d'équipe
- Instaurer des rituels
  - Echanges de décompression post-incident pour remonter les problèmes humains et émotionnels
  - Evènements d'équipe
  - Déployer davantage de mesures de cohésion d'équipe, afin de garantir des échanges hors périodes de stress
- Visibiliser les spécificités liées aux SOC et CERT
  - Insister, notamment dans les échanges avec d'autres managers, sur le caractère unique et exceptionnel du rythme SOC et CERT
  - Assurer la visibilité (par des réunions dédiées ou de la vulgarisation) des spécificités du métier aux autres équipes et services.

Pour les collaborateurs et collaboratrices

- Ouvrir la possibilité d'échanger post-incident sur les difficultés humaines rencontrées. Un incident est très souvent un catalyseur des problématiques interpersonnelles au sein des équipes, et ces conflits peuvent avoir un poids fort sur la santé mentale des collègues.
- Assurer autant que possible un binômage sur les incidents et alertes
- Réfléchir à recréer du sens pour éviter les phénomènes d'aliénation et de décrochage.
- Mettre en place des mécanismes de relais sur les incidents longs.

CONCLUSION

Cette étude nationale menée en 2024 par InterCERT France sur les risques psychosociaux (RPS) dans les environnements CERT et SOC met en lumière plusieurs constats majeurs et axes de progrès essentiels.

Le rythme de travail unique et la pression constante inhérente aux CERT et SOC génèrent un stress particulier, qui nécessite une reconnaissance spécifique tant en interne qu'auprès des autres équipes et services. La visibilité et la valorisation des spécificités de ces métiers apparaissent comme des leviers indispensables pour améliorer la compréhension mutuelle et renforcer la considération de ces équipes.

L'importance d'instaurer des mesures de cohésion en dehors des périodes de stress est soulignée, afin de consolider les liens et d'offrir des espaces d'échanges plus sereins. Ouvrir la possibilité de débriefer collectivement après un incident, notamment sur les aspects humains, permet d'anticiper et de limiter l'impact des conflits interpersonnels sur la santé mentale des collaborateurs et collaboratrices. De plus, la systématisation du binômage lors d'incidents ou d'alertes contribue à réduire l'isolement et à mieux répartir la charge émotionnelle.

Les résultats de l'étude rappellent également la nécessité de repenser l'organisation du travail et le sens donné aux missions, afin de prévenir les phénomènes d'aliénation ou de décrochage professionnel. La mise en place de mécanismes de relais pour la gestion des incidents prolongés s'impose comme une bonne pratique pour préserver l'engagement et la santé des équipes. Enfin, l'ensemble de ces recommandations s'inscrit dans une démarche globale d'amélioration de la qualité de vie au travail, de résilience collective et de performance durable.

En synthèse, la prise en compte des spécificités du métier, la valorisation des échanges humains et le renforcement du soutien organisationnel constituent les piliers d'une stratégie efficace de prévention des RPS dans les CERT et SOC. Il appartient désormais à chaque structure de s'approprier ces leviers pour bâtir un environnement de travail plus sain, solidaire et attractif, au bénéfice de l'ensemble de la communauté cyber.

InterCERT
FRANCE

InterCERT France
Campus Cyber, Tour Eria
5-7 rue Bellini
92800 PUTEAUX
contact@intercert-france.fr
07 52 08 04 21

Conception graphique www.aurelielegrand.fr