SOPHOS

LE COÛT HUMAIN DE LA VIGILANCE : LUTTER CONTRE L'ÉPUISEMENT PROFESSIONNEL LIÉ À LA CYBERSÉCURITÉ EN 2025

Un livre blanc Sophos. Août 2025

Introduction

Le paysage de la cybersécurité est de plus en plus caractérisé par la pression incessante exercée par des cybermenaces sophistiquées, notamment les ransomwares. Face à l'omniprésence des menaces, les équipes informatiques et de cybersécurité doivent composer avec des exigences de plus en plus élevées, ce qui entraîne des problèmes de plus en plus importants de fatigue et de burn-out.

Ce rapport examine l'impact humain direct de ces pressions, en s'appuyant sur de nouvelles données de recherche. Il met en évidence la prévalence, les principaux facteurs et les conséquences du burn-out, et fait état de solutions stratégiques permettant de remédier à ce problème critique.

Les données ont été recueillies dans le cadre d'une enquête menée auprès de 5 000 professionnels de l'IT et de la cybersécurité à travers 17 pays. Dans le cadre de cette enquête, menée au premier trimestre 2025, les personnes interrogées ont été invitées à réfléchir à leurs expériences au cours des 12 derniers mois.

Comprendre les phénomènes de fatigue et d'épuisement professionnel liés à la cybersécurité

La fatigue liée à la cybersécurité se caractérise[1] par un état d'épuisement psychique et émotionnel, souvent consécutif à une vigilance constante, à un trop grand nombre d'alertes à gérer et à la nature hautement délicate de la défense contre des cybermenaces en constante évolution. Elle traduit l'épuisement cognitif et émotionnel dont souffrent les professionnels de ce domaine particulièrement exigeant.

Le burn-out est un syndrome psychologique plus généralisé qui se caractérise par un épuisement émotionnel, un cynisme et une diminution du sentiment d'accomplissement personnel, découlant souvent d'un stress chronique au travail. Dans le domaine de la cybersécurité, la fatigue peut être envisagée comme une manifestation directe ou un facteur contribuant de manière significative à un burn-out plus général.

Le burn-out lié à la cybersécurité est une manifestation spécifique de ce concept plus large d'épuisement professionnel dans le contexte particulier du monde de la cybersécurité. Il englobe l'épuisement psychique, physique et émotionnel résultant d'une exposition excessive et prolongée aux pressions inhérentes au travail dans le domaine de la cybersécurité.

Les professionnels de ce domaine doivent répondre à des attentes cognitives et émotionnelles uniques, notamment la gestion constante des alertes de sécurité, la nécessité de respecter des réglementations strictes et la rapidité de réponse requise face aux cybermenaces émergentes.

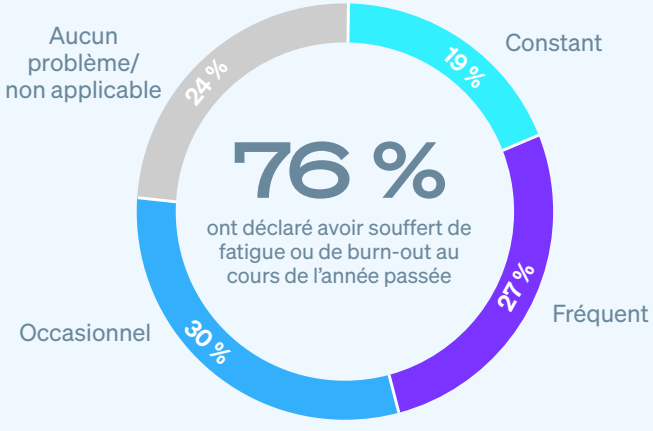
Cette exposition continue à des tâches impliquant une très forte pression et la nécessité d'apporter des réponses rapides et précises aux incidents sont autant de facteurs fondamentaux qui amplifient le risque de fatigue et de burn-out chez les professionnels de la cybersécurité.

Tensions persistantes et répercussions importantes

Les expériences du burn-out

La pression exercée sur les professionnels de la cybersécurité est évidente au vu des répercussions généralisées auxquelles ont été confrontées les équipes IT et de cybersécurité au cours de l'année écoulée.

76 % des personnes interrogées sur leur expérience personnelle de la fatigue ou du burn-out ont déclaré en avoir fait eux-mêmes l'expérience au cours de l'année passée. Plus précisément, pour 19 % il s'agissait d'un problème « constant », pour 27 % d'un problème « fréquent » et pour 30 % d'un problème « occasionnel ».



Avez-vous ressenti de la fatigue ou un burn-out lié à la cybersécurité au cours de l'année écoulée ? n = 5 000

[1]Détox numérique : exploration de l'impact de la fatigue liée à la cybersécurité sur la productivité et la santé mentale des employés

Les données révèlent que le burn-out est un phénomène omniprésent, indépendamment de la taille de l'organisation : 76 % des répondants dans les entreprises comptant entre 100 et 1 000 employés, 77 % dans celles comptant entre 1 001 et 3 000 employés et 75 % dans les celles comptant entre 3 001 et 5 000 employés ont traversé une phase de burn-out.

Pire, le problème semble bien s'aggraver :
69 % des répondants ont déclaré que la fatigue et le burn-out liés à la cybersécurité avaient augmenté entre 2023 et 2024.

Les conséquences du burn-out

Sans surprise, l'épuisement professionnel a des incidences négatives importantes sur les salariés qui en souffrent : près de la moitié (46 %) d'entre eux déclarent ressentir une anxiété accrue à l'idée de subir une cyberattaque ou une violation de données, quatre sur dix (39 %) admettent avoir vu leur productivité diminuer au travail et un tiers (33 %) affirment se sentir moins impliqué dans leur travail.

Conséquences de la fatigue et du burn-out liés à la cybersécurité

Impact du burn-out	Moyenne (n=3 803)	Niveau de burn-out ressenti		
		Problème constant (n=944)	Problème fréquent (n=1 357)	Problème occasionnel (n=1 502)
Ont ressenti une anxiété accrue face aux cyberattaques ou aux violations de données	**46 %**	47 %	45 %	46 %
Ont constaté une baisse de la productivité au travail	**39 %**	36 %	36 %	43 %
Ont constaté une baisse du niveau d'engagement au travail	**33 %**	34 %	33 %	34 %
Ont ressenti le besoin de prendre un congé	**29 %**	31 %	28 %	28 %
Ont envisagé de changer de carrière/de poste	**23 %**	29 %	25 %	17 %
Ont envisagé de démissionner	**22 %**	28 %	25 %	16 %

Quelles ont été les conséquences personnelles de la fatigue ou du burn-out liés à la cybersécurité, le cas échéant ? Répondants ayant déclaré avoir souffert un burn-out au cours des 12 derniers mois. Chiffres de base dans le graphique.

Ces chiffres témoignent d'un phénomène courant qui nuit directement à l'efficacité et à la durabilité des défenses en matière de cybersécurité.

Causes principales des tensions

La nature exigeante des cyberdéfenses modernes, exacerbée par le rythme incessant des cyberattaques, contribue considérablement à l'épuisement professionnel. Parmi tous les répondants du secteur de la cybersécurité ayant déclaré avoir ressenti de la fatigue ou un burn-out, les changements constants dans les technologies/solutions de cyberdéfense étaient le facteur contributif le plus courant (38 %). Pour ceux pour lesquels le burn-out est un problème « constant », c'est la nature même du travail dans le domaine de la cybersécurité — à savoir des tâches routinières entrecoupées d'activités nécessitant une grande concentration — qui en est la cause la plus fréquente, citée par 40 % des personnes interrogées.

Conséquences de la fatigue et du burn-out liés à la cybersécurité

Cause du burn-out	**Moyenne** (n=3 803)	Niveau de burn-out ressenti		
		Problème constant (n=944)	**Problème fréquent** (n=1 357)	**Problème occasionnel** (n=1 502)
Changements constants au niveau des technologies/ solutions de cyberdéfense	**38 %**	36 %	37 %	41 %
La nature des activités liées à la cybersécurité (tâches routinières entrecoupées d'activités ciblées)	**37 %**	40 %	36 %	36 %
Évolution constante des menaces	**34 %**	31 %	31 %	39 %
La nécessité d'une couverture 24/7	**32 %**	30 %	32 %	33 %
Pression découlant de l'évolution des obligations réglementaires et légales	**32 %**	34 %	34 %	29 %
Changements constants dans les priorités	**30 %**	28 %	29 %	32 %
Pression exercée par le conseil d'administration et/ou la direction générale	**30 %**	29 %	30 %	30 %
Manque de personnel qualifié	**27 %**	24 %	26 %	29 %
Restrictions budgétaires (excluant la dotation en personnel)	**26 %**	27 %	28 %	24 %
Manque d'accès à une assistance tierce spécialisée	**26 %**	30 %	25 %	23 %
Volume élevé d'alertes	**25 %**	24 %	26 %	25 %

Quels facteurs ont été à l'origine de la fatigue/du burn-out liés à la cybersécurité que vous avez ressentis ? Répondants ayant déclaré avoir souffert un burn-out au cours des 12 derniers mois. Chiffres de base dans le graphique.

En moyenne, les répondants ont cité trois facteurs distincts ayant contribué à leur épuisement professionnel, mettant en évidence les multiples pressions auxquelles sont soumises les équipes IT.

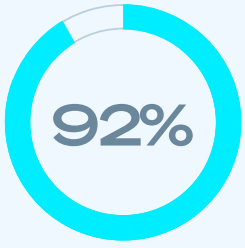
Impact individuel et organisationnel

Un burn-out non géré a des répercussions négatives en cascade, qui affectent non seulement le bien-être individuel des professionnels de la sécurité, mais aussi la résilience globale de l'organisation.

- **Impact individuel :** les professionnels éprouvent un stress accru, de l'anxiété, une moindre satisfaction professionnelle et des effets néfastes sur leur santé mentale et physique. Cela peut également créer des tensions entre les individus et entraîner une augmentation du taux de rotation du personnel.
- **Impact organisationnel :**
  - Vulnérabilité accrue : les équipes épuisées ont davantage tendance à commettre des erreurs et à faire des oublis, ce qui peut engendrer des failles de sécurité critiques et augmenter le risque de violations réussies.
  - Efficacité réduite : le burn-out a des effets négatifs sur la concentration, les prises de décision et la productivité, compromettant ainsi la capacité de l'équipe à se défendre contre les menaces avancées.
  - Réduction naturelle des effectifs : le stress élevé associé à cette fonction contribue à un roulement important de professionnels qualifiés, ce qui aggrave la pénurie actuelle de talents en matière de cybersécurité.
  - Perturbation opérationnelle : une posture de sécurité compromise en raison de l'épuisement professionnel peut entraîner des incidents de sécurité plus fréquents et plus graves, notamment des attaques de ransomware, pouvant eux-mêmes générer des temps d'arrêt opérationnels et des pertes financières importantes.

Mesures stratégiques et leur efficacité

Les organisations déploient diverses stratégies pour atténuer la fatigue professionnelle liée à la cybersécurité. S'il est vrai que la mise en place de diverses mesures internes est bénéfique (comme la promotion d'une culture de soutien, la mise à disposition de ressources en matière de santé mentale et l'investissement dans le développement professionnel), l'adoption de partenariats externes stratégiques, en particulier le recours à des services MDR (Managed Detection and Response, détection et réponse managées), apparaît tout à fait pertinente.



des répondants concernés qui utilisent un service MDR affirment que leur fatigue et leur épuisement liés à la cybersécurité s'en sont trouvés réduits.

L'étude révèle que les services MDR constituent un moyen très efficace d'atténuer l'épuisement professionnel : 92 % des répondants concernés qui utilisent un tel service affirment que celui-ci a réduit leur niveau de fatigue et de burn-out en matière de cybersécurité. Parmi ceux pour qui le burn-out est un problème « constant », la moitié fait état d'une réduction « significative » et 45 % supplémentaires affirment que le service a « légèrement » réduit leur niveau d'épuisement professionnel. Ces résultats témoignent d'un large consensus autour de l'idée que le fait de confier les opérations de sécurité critiques à des prestataires experts de services MDR réduit considérablement la pression exercée sur les équipes internes.

Efficacité des services MDR dans la réduction de la fatigue et du burn-out liés à la cybersécurité

Impact :	Moyenne (n=3 750)	Niveau de burn-out ressenti		
		Problème constant (n=940)	Problème fréquent (n=1 340)	Problème occasionnel (n=1 470)
Réduction significative du burn-out	**39 %**	50 %	35 %	34 %
Réduction légère du burn-out	**53 %**	45 %	56 %	56 %
Total	**92 %**	95 %	92 %	90 %

Si votre organisation utilise un service managé de détection et réponse (MDR), celui-ci a-t-il contribué à réduire la fatigue ou le burn-out liés à la cybersécurité ? Répondants ayant déclaré avoir fait l'objet d'un burn-out au cours des 12 derniers mois et dont l'organisation utilise un service MDR. Chiffres de base dans le graphique.

Sophos MDR, pilier d'une défense durable

La lutte contre la cybercriminalité ne connaît pas de répit. Pour mettre en place une défense véritablement résiliente, les organisations doivent non seulement renforcer leurs capacités technologiques, mais aussi garantir le bien-être des personnes impliquées dans les activités de cyberdéfense.

Sophos MDR constitue une solution convaincante pour réduire le burn-out lié à la cybersécurité en s'attaquant à un grand nombre de ses causes fondamentales :

- **Apprentissage continu :** l'équipe Sophos MDR est très au fait des innovations en matière de technologies de cyberdéfense et de menaces, pour s'assurer que ses clients profitent pleinement des avancées technologiques et optimisent leurs défenses.
- **Surveillance continue et réponse immédiate aux attaques :** les analystes experts de Sophos MDR assument pour le compte de leurs clients la nature imprévisible des opérations de sécurité : surveillance continue, détection et investigation, tâches qui consomment une bande passante importante, mais aussi réponse complète aux menaces en cas d'incident, ce qui évite aux équipes internes de devoir intervenir en urgence (souvent en dehors des heures de bureau).
- **Accès direct à des experts en sécurité :** les clients de Sophos MDR peuvent compter sur l'expertise de centaines d'analystes dans tous les domaines liés à la sécurité, notamment des spécialistes de la chasse aux menaces, de la détection, de l'investigation et de la réponse, ainsi que des experts en malwares et en acteurs malveillants travaillant en coulisses.
- **Couverture 24/7 :** sept centres opérationnels de sécurité mondiaux assurent une couverture continue, garantissant ainsi une protection totale aux clients à toute heure du jour et de la nuit.
- **Triage des alertes assisté par IA :** le volume considérable d'alertes de sécurité peut rapidement s'avérer déconcertant.

  Sophos MDR combine des outils de triage sur mesure assistés par IA et une expertise humaine approfondie pour repérer rapidement les activités suspectes parmi le bruit ambiant.

En s'associant à Sophos MDR, les entreprises sont en mesure d'instaurer une posture de sécurité robuste et proactive qui non seulement renforce leurs défenses contre les menaces, telles que les ransomwares, mais soutient également de manière cruciale le bien-être tant mental que professionnel de leurs experts en cybersécurité, garantissant ainsi une défense humaine durable et efficace face aux cybermenaces en constante évolution.

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses, contactez un conseiller ou visitez le site www.sophos.fr

Apprenez-en plus sur les ransomwares et sur la façon dont Sophos peut vous aider à protéger votre organisation.

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2025-08-26 WP (MP)

SOPHOS