orca security

Rapport concernant la fatigue d'alerte pour la sécurité cloud 2022

L'échelle de la fatigue des alertes pour le cloud public, ses causes, les impacts et les solutions possibles

Dans ce rapport

Résumé

Les professionnels de la sécurité ne connaissent que trop bien la fatigue des alertes. Ils y ont été confrontés dans le monde sur site, et maintenant ils y sont confrontés dans le cloud. Les organisations utilisent de nombreux outils de sécurité différents qui génèrent chacun des alertes, ce qui surcharge les équipes de sécurité qui doivent passer des heures chaque jour à examiner les alertes pour déterminer quels problèmes doivent être résolus en premier.

Comme dans l'histoire du « garçon qui criait au loup », si le nombre d'alertes inutiles et faussement positives devient trop important, les intervenants se désensibilisent, ce qui fait que des alertes qui méritent vraiment une attention particulière passent inaperçues.

Résumé

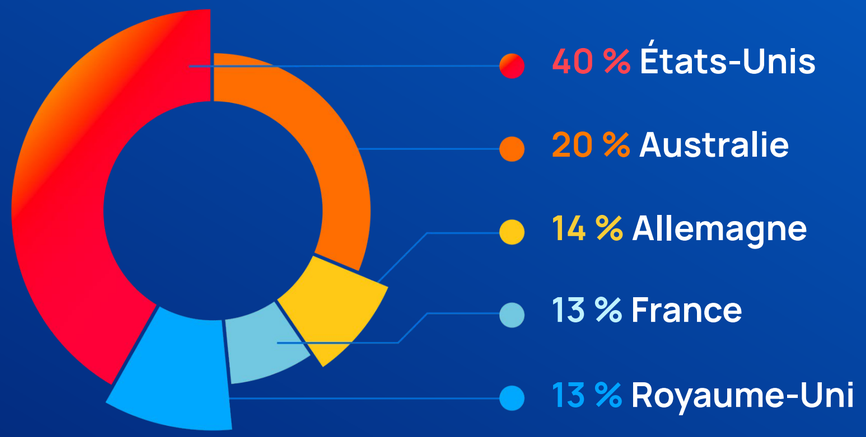
L'enquête

Pour en savoir plus sur l'état actuel de la fatigue des alertes, ses causes, ses impacts et les solutions possibles, Orca Security a commandé une enquête mondiale auprès de 813 décideurs informatiques dans cinq pays et dans dix industries.

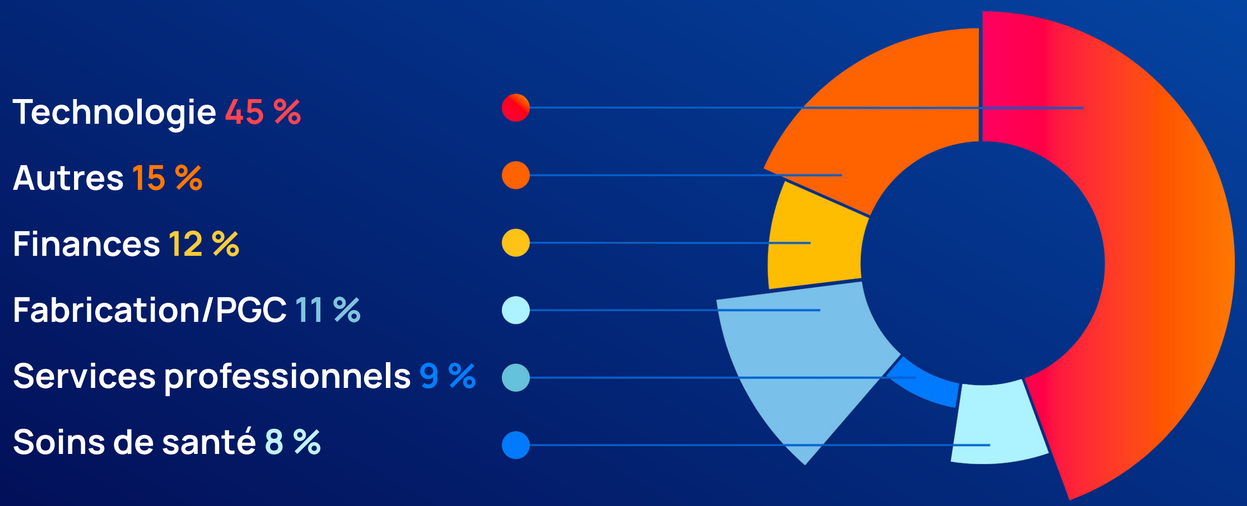
Ce rapport présente les résultats globaux. Les principaux résultats par pays et par secteur d'activité sont énumérés dans l'annexe.

> La majorité des personnes interrogées provenaient d'entreprises comptant **200 à 1000 employés** (79 %).
>
> Les équipes de sécurité cloud de la plupart des personnes interrogées sont composées de **1 à 50 membres**.

Pays



Secteur d'activité



Résumé

Les personnes interrogées

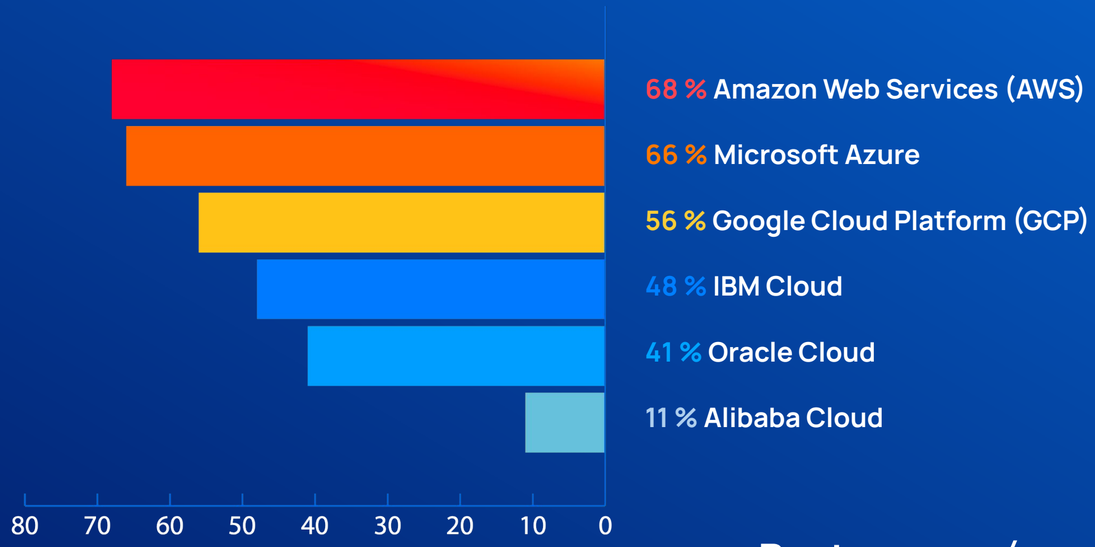
Pour participer à l'enquête, les personnes interrogées devaient disposer d'au moins 25 actifs cloud sur l'une des principales plateformes de cloud public. La majorité des personnes interrogées (84 %) comptait plus de 100 actifs cloud. La plupart des personnes interrogées utilisent AWS, Azure et Google Cloud, suivis de près par IBM Cloud et Oracle Cloud.

Les postes qu'occupaient les personnes interrogées allaient de celui d'employé (10 %) à celui de cadre (29 %), en passant par celui de gestionnaire (61 %).

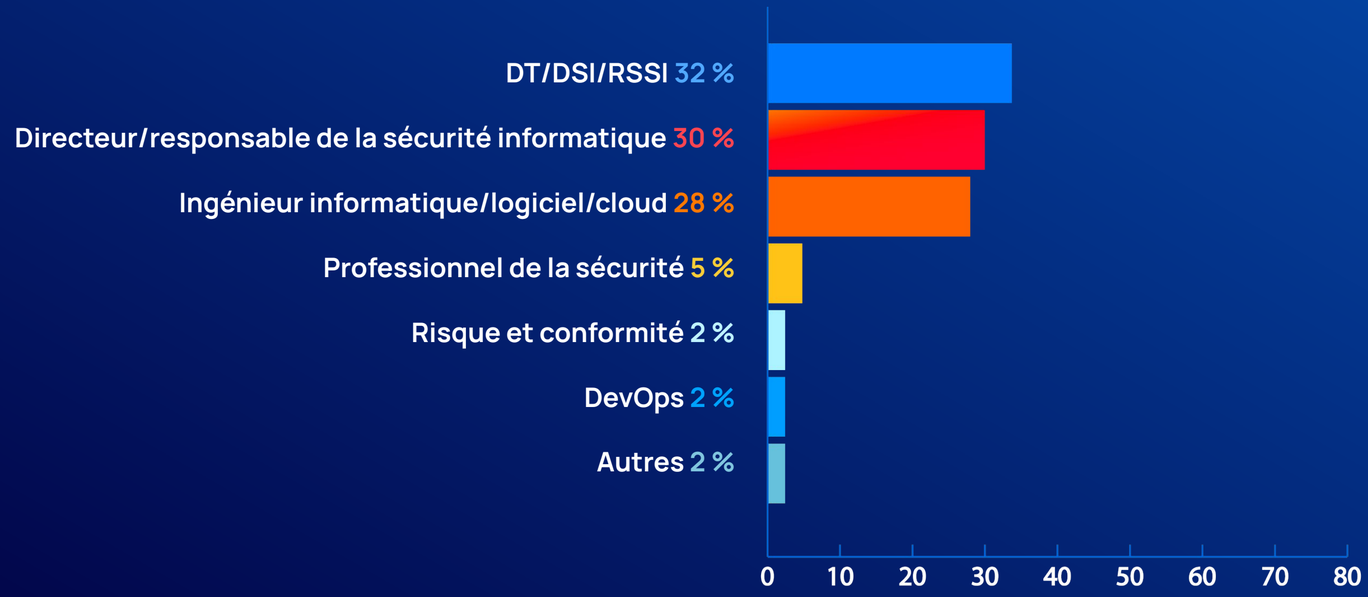
La vaste majorité (81 %) utilise une **stratégie multicloud** avec plus d'une plateforme cloud.

55 % des personnes interrogées utilisent 3 plateformes de cloud public **ou plus**

Plateformes de cloud public utilisées



Poste occupé



Résumé

Principales conclusions

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 59 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 43 % déclarent que plus de 40 % de leurs alertes sont des faux positifs et 49 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 56 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement professionnel, la rotation du personnel et des frictions internes :** 62 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel et 60 % ont déclaré que la fatigue des alertes a créé des frictions internes.
- **Des alertes critiques sont manquées, souvent sur une base quotidienne ou hebdomadaire :** parmi les 55 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 41 % ont déclaré que les alertes sont manquées hebdomadairement et 22 % ont déclaré qu'elles sont manquées quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 57 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 95 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 43 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 97 % des personnes interrogées se déclarent **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 49 % déclarent que plus de 40 % des alertes sont de faible priorité.

59 %

reçoivent plus de 500 alertes de sécurité cloud par jour

62 %

déclarent que la fatigue des alertes a contribué à la rotation du personnel

95 %

font confiance à la précision de leurs outils de sécurité ?

1

Les équipes de sécurité sont inondées par des alertes

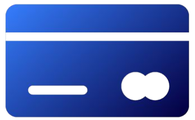
Les équipes de sécurité sont inondées d'alertes chaque jour. 59 % des personnes interrogées reçoivent plus de 500 et 38 % plus de 1000 alertes de sécurité relatives au cloud public par jour. En plus de recevoir de nouvelles alertes, les équipes doivent également gérer les alertes en cours de correction et qui n'ont pas encore été clôturées. 79 % des personnes interrogées ont déclaré avoir plus de 500 alertes de sécurité du cloud ouvertes à un moment donné et 55 % ont déclaré en avoir plus de 1000.

Une grande partie de la journée d'un professionnel de la sécurité est consacrée à examiner et à hiérarchiser les alertes. Plus de la moitié des équipes de sécurité ont déclaré passer plus de 20 % de leur temps et un quart des équipes passent plus de 40 % de leur temps à décider quelles alertes devraient être traitées en premier.

Une journée dans la vie d'un professionnel de la sécurité :

- **59 %** reçoivent plus de 500 alertes de sécurité cloud par jour
- **56 %** passent plus de 20 % de leur journée à examiner et à hiérarchiser les alertes
- **79 %** ont plus de 500 alertes de sécurité cloud ouvertes quotidiennement

Le secteur financier souffre le plus



71 % des personnes interrogées dans les services financiers reçoivent plus de 500 alertes de sécurité dans le cloud public par jour, **85 %** ont plus de 500 alertes de sécurité dans le cloud public et **63** % des équipes de sécurité passent plus de 20 % de leur temps à examiner et à hiérarchiser les alertes chaque jour.
Cela indique que les contrôles de sécurité et de conformité sont plus élevés pour le secteur des services financiers.

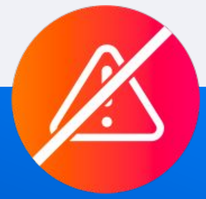
2

Les alertes manquent de précision

Les équipes de sécurité reçoivent de nombreux problèmes signalés à tort. Pas moins de 81 % des personnes interrogées affirment que plus de 20 % des alertes sont des faux positifs.
Un peu moins de la moitié (43 %) a déclaré que plus de 40 % de leurs alertes sont des faux positifs. Quoi qu'il en soit, les équipes doivent traiter chaque alerte comme s'il s'agissait d'un vrai positif jusqu'à ce qu'elles sont sûres du contraire. Cette situation entraîne une perte de temps et contribue à la désensibilisation.

Même si les alertes ne sont pas des faux positifs, mais des alertes de faible priorité qui ne doivent pas être traitées immédiatement, elles font perdre du temps si les équipes doivent les séparer des alertes importantes. 49 % des personnes interrogées déclarent que plus de 40 % des alertes sont de faible priorité et pas moins de 83 % déclarent que plus de 20 % de leurs alertes sont de faible priorité.

Seul un petit nombre d'alertes sont en fait critiques et nécessitent une attention immédiate, moins de 10 %, en fait, pour la majorité des personnes interrogées. Toutefois, pour trouver ces 10 % d'alertes parmi les centaines d'alertes de faible priorité et de faux positifs, les équipes doivent consacrer beaucoup de temps à l'analyse et à l'investigation des alertes.



Le garçon qui criait au loup ?

43 %

déclarent que plus de 40 % de leurs alertes sont des faux positifs

49 %

déclarent que plus de 40 % sont des alertes de faible priorité

64 %

déclarent que moins de 10 % des alertes sont critiques

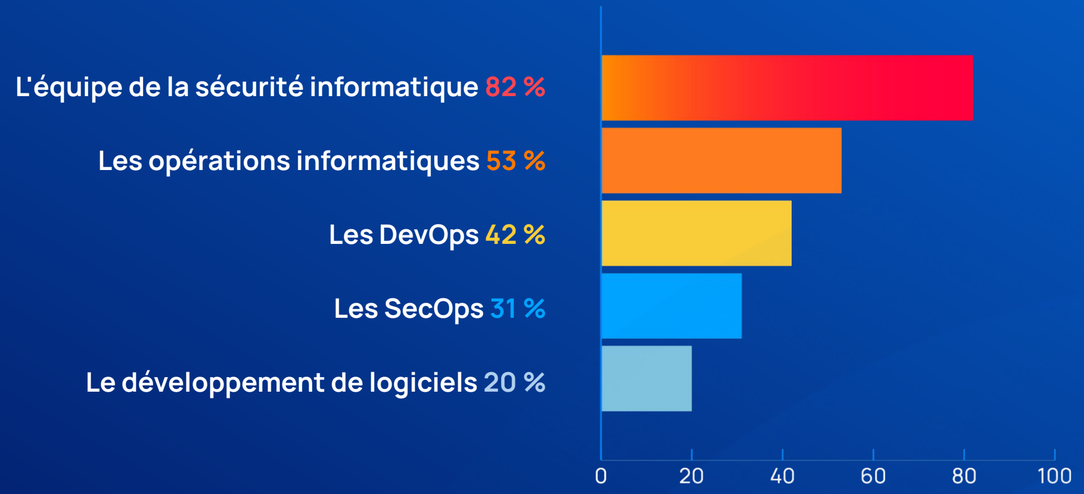
3

Le fardeau de la correction incombe aux équipes de sécurité

En plus de décider quelles alertes doivent être hiérarchisées, les équipes de sécurité ont la plus grande responsabilité dans le triage et la correction des alertes, 82 % des personnes interrogées citent l'équipe de sécurité informatique et 31 % les SecOps comme groupe responsable de la correction des alertes. Le développement de logiciels semble être le moins souvent sollicité, avec seulement 20 % des personnes interrogées désignant le développement comme responsable de la correction.

Beaucoup de problèmes de sécurité cloud ne sont pas faciles à corriger. Seules 19 % des personnes interrogées ont déclaré qu'il fallait en moyenne moins d'un jour pour corriger une alerte. 35 % ont déclaré d'un à deux jours et près de la moitié des personnes interrogées ont déclaré que la correction prenait trois jours ou plus.

Qui est responsable du triage et de la correction des alertes ?



Les équipes de sécurité supportent également la plus grande partie du fardeau de la correction

82 %

déclarent que l'équipe de sécurité informatique est responsable de la correction des alertes

46 %

ont déclaré qu'il fallait 3 jours ou plus pour corriger une alerte

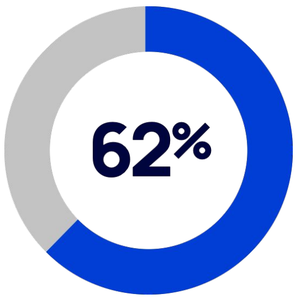
79 %

ont plus de 500 alertes de sécurité cloud ouvertes quotidiennement

4

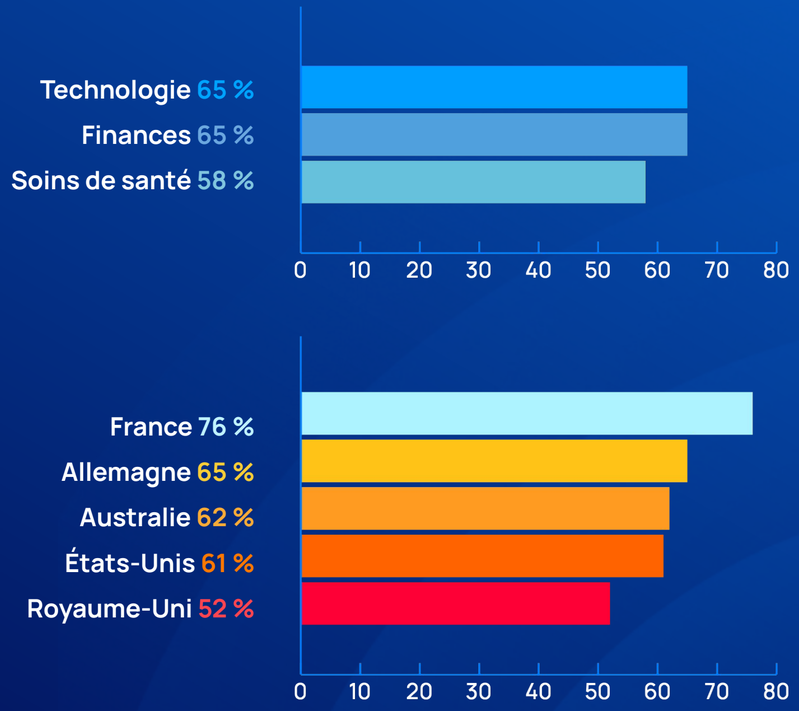
Les équipes de sécurité s'épuisent

Compte tenu du nombre d'alertes, des nombreux faux positifs et des alertes de faible priorité, et du petit nombre d'alertes qui nécessitent réellement une attention, les équipes sont démoralisées, surmenées et épuisées. **62 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel dans leur organisation**. Quel que soit le pays ou le secteur d'activité, la majorité des personnes interrogées déclarent toutes que la fatigue des alertes a conduit le personnel à quitter son poste. Toutefois, le Royaume-Uni semble se situer au bas de l'échelle et la France semble être la plus touchée par le problème.



des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel dans leur organisation.

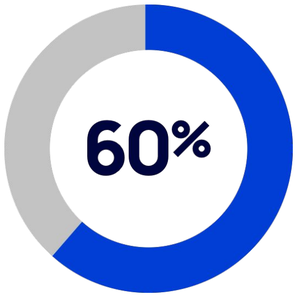
La majorité déclare que la fatigue des alertes a contribué à la rotation du personnel :



5

La fatigue des alertes conduit à la friction interne

Comme la correction des alertes est souvent une responsabilité partagée entre la sécurité, l'informatique et les DevOps, la fatigue des alertes affecte également la coopération interne au sein de l'organisation. **60 % des personnes interrogées ont déclaré que la fatigue des alertes avait créé des frictions entre leurs équipes DevOps et de sécurité**.



des personnes interrogées ont déclaré que la fatigue des alertes avait créé des frictions entre leurs équipes DevOps et de sécurité.

La majorité déclare que la fatigue des alertes a créé des frictions organisationnelles :

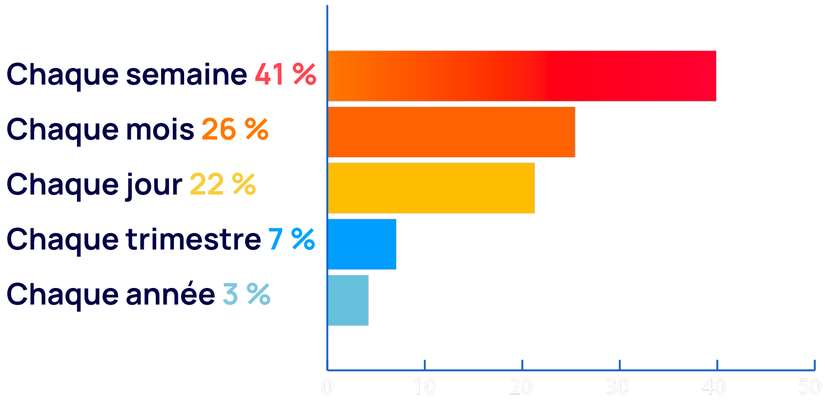
6

Des alertes critiques sont manquées

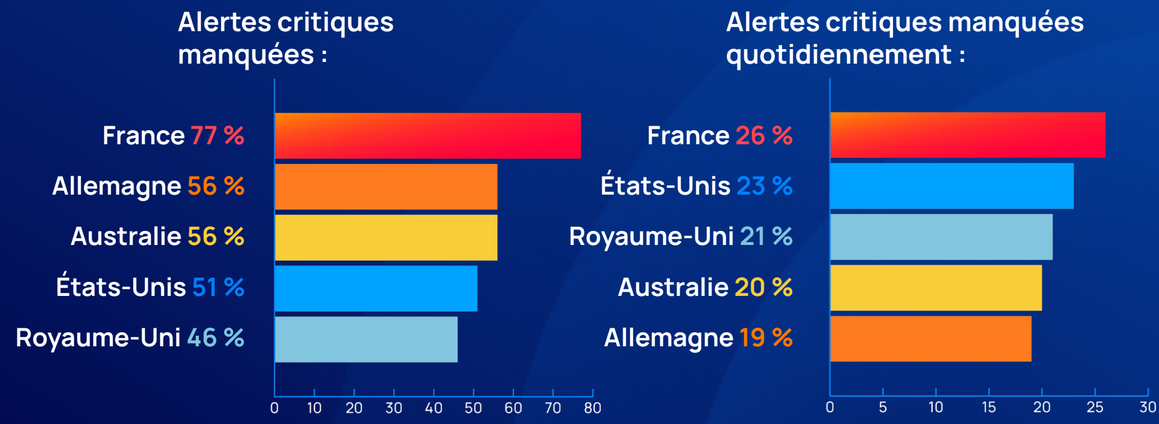
En raison du nombre considérable d'alertes qui ne sont pas prioritaires, les professionnels de la sécurité se désensibilisent, si bien que les alertes qui nécessitent une attention immédiate passent inaperçues, ce qui peut avoir des conséquences désastreuses.

> Plus de la moitié des personnes interrogées (55 %) ont déclaré que leur équipe a manqué des alertes critiques dans le passé dues à une hiérarchisation des alertes inefficaces. Parmi ces personnes interrogées, 22 % ont déclaré qu'elles manquaient des alertes critiques chaque jour, 41 % chaque semaine et 26 % chaque mois.

Alertes critiques souvent négligées



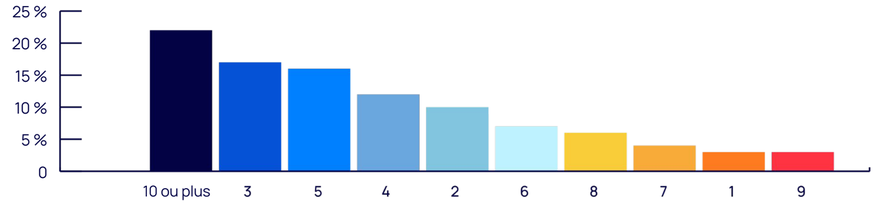
Par pays



7

Des outils de sécurité compartimentés qui exacerbent le problème

La grande majorité des personnes interrogées utilisent au moins trois outils de sécurité pour le cloud public (87 %) et 57 % en utilisent cinq ou plus. Les types d'outils les plus utilisés sont les outils d'analyse du réseau (84 %), suivis de près par les outils de sécurité natifs de la plateforme cloud (82 %).



Nombre d'outils de sécurité dans le cloud public

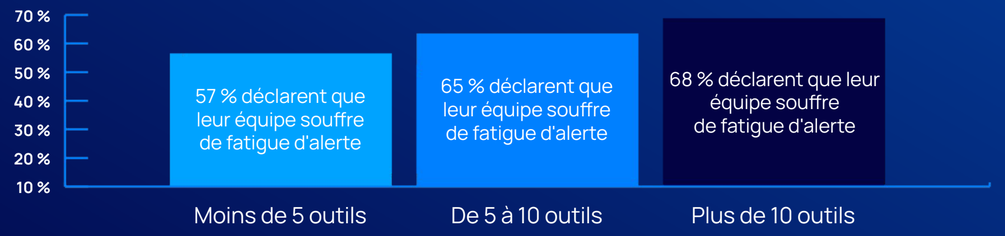
Les données montrent que plus les équipes de sécurité déploient d'outils, plus elles reçoivent d'alertes. Cette corrélation peut s'expliquer en partie par le fait que les grandes entreprises ont tendance à disposer de plus d'outils de sécurité, et probablement aussi de plus de ressources cloud pour lesquelles des alertes sont générées. Toutefois, le fait que plusieurs outils signalent certains problèmes indentiques constitue sans aucun doute un autre facteur contributif.

Il est intéressant de noter que la proportion de faux positifs semble également augmenter avec le nombre d'outils, de même que le problème de la fatigue des alertes, qui semble à nouveau indiquer que plusieurs outils signalent les mêmes problèmes, créant ainsi un travail en double pour les équipes de sécurité.

Plus d'outils = Plus d'alertes

Plus d'outils = Plus de faux positifs ?

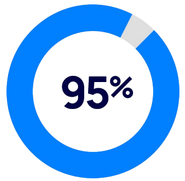
Plus d'outils = Plus de fatigue des alertes ?



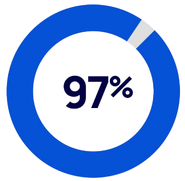
8

La barre des outils de sécurité est-elle placée trop bas ?

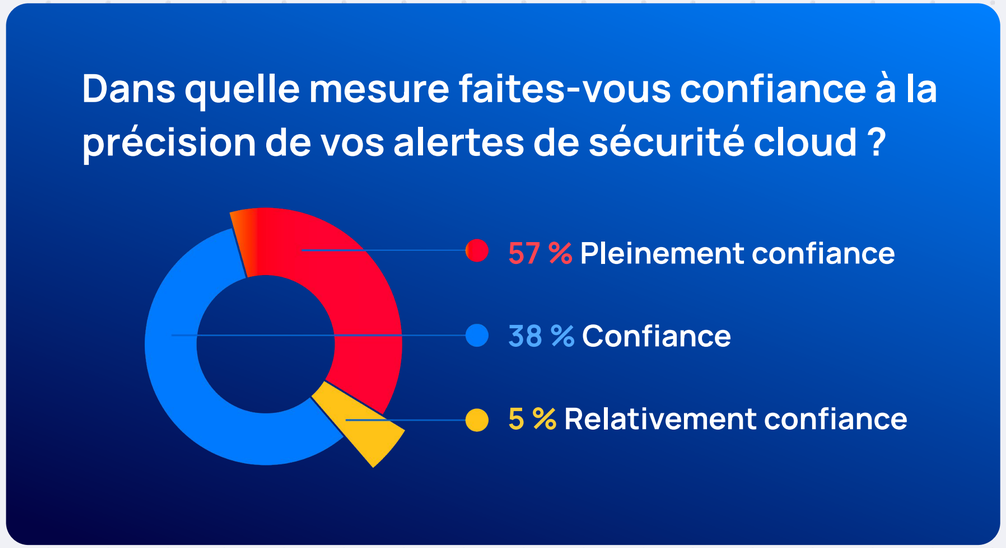
La grande majorité des personnes interrogées déclarent être satisfaites et faire confiance à la hiérarchisation des alertes et la précision de leurs outils de sécurité. Toutefois, nos recherches montrent que cette confiance n'est peut-être pas entièrement méritée. Nos personnes interrogées placent-elles la barre trop bas ?

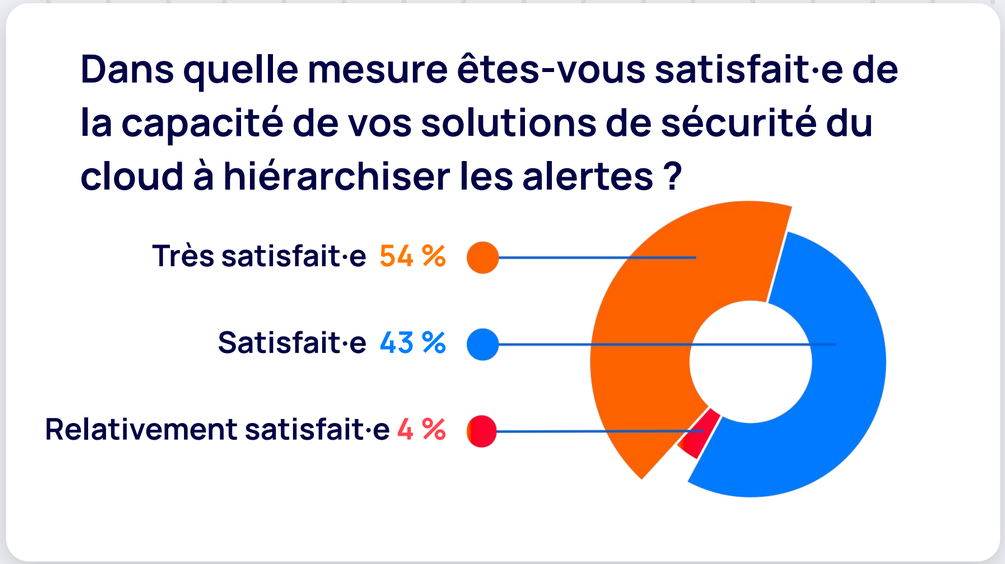


95 % des personnes interrogées déclarent faire confiance ou pleinement confiance à la précision de leurs outils de sécurité, cependant, 40 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.



97 % des personnes interrogées se déclarent satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques, même si 49 % d'entre elles déclarent que plus de 40 % des alertes sont de faible priorité.





9

Principales recommandations

L'enquête montre que la fatigue des alertes est un problème majeur pour la plupart des équipes de sécurité du cloud. Cette situation entraîne non seulement une rotation du personnel, mais aussi l'absence d'alertes critiques, souvent hebdomadairement, voire quotidiennement. L'utilisation de plusieurs outils compartimentés pour signaler les alertes de sécurité du cloud crée des alertes en double et augmente inutilement la charge des équipes de sécurité déjà surchargées.

Que peuvent donc faire les organismes pour résoudre le problème de la fatigue des alertes ? Les organismes doivent donner aux équipes de sécurité les moyens de travailler mieux, et non pas plus.

Consolidation des outils : au lieu d'ajouter d'autres outils compartimentés, consolidez les outils dans un plus petit nombre de plateformes afin d'éviter les alertes en double et d'améliorer la hiérarchisation des risques en exploitant les informations contextuelles centralisées pour découvrir les combinaisons de risques dangereuses.

Exigez davantage de vos outils de sécurité : demandez aux fournisseurs de sécurité comment ils hiérarchisent les risques. Assurez-vous qu'ils combinent de nombreux facteurs tels que la gravité, la facilité d'exploitation, l'accessibilité et l'impact potentiel sur l'entreprise.

Protégez la cible plutôt que le point d'entrée : assurez-vous de savoir où se trouvent vos actifs les plus critiques et vérifiez si votre fournisseur de sécurité hiérarchise automatiquement les risques en fonction de l'exposition potentielle de ces actifs.

Concentrez-vous sur les voies d'attaque : les équipes de sécurité doivent passer de l'examen d'alertes compartimentées à l'examen et à la hiérarchisation des chaînes d'attaques afin d'obtenir un aperçu plus rapide des problèmes à résoudre en priorité.

Correction stratégique : au lieu d'essayer de réparer toutes les alertes dans la chaîne d'attaque, commencez par corriger celle qui brise la chaîne pour endiguer le danger le plus immédiat.

Annexe

Principales conclusions
Etats-Unis

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 61 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 48 % déclarent que plus de 40 % de leurs alertes sont des faux positifs et 54 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 63 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement, la rotation du personnel et la friction interne :** 61 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel et 57 % ont déclaré que la fatigue des alertes a créé une friction interne.
- **Des alertes critiques sont manquées, souvent quotidiennement ou hebdomadairement :** parmi les 51 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 37 % ont déclaré que les alertes sont manquées hebdomadairement et 23 % ont déclaré qu'elles sont manquées quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 58 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 95 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 48 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 96 % des personnes interrogées se déclarent **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 54 % d'entre elles déclarent que plus de 40 % des alertes sont de faible priorité.

61 %

reçoivent plus de 500 alertes de sécurité cloud par jour

61 %

indiquent que la fatigue des alertes a contribué à la rotation du personnel

95 %

font confiance à la précision de leurs outils de sécurité ?

Principales conclusions

Royaume-Uni

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 53 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 45 % déclarent que plus de 40 % de leurs alertes sont des faux positifs et 54 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 52 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement, la rotation du personnel et la friction interne :** 52 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel et 56 % ont déclaré que la fatigue des alertes a créé une friction interne.
- **Des alertes critiques sont manquées, souvent quotidiennement ou hebdomadairement :** parmi les 46 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 46 % ont déclaré que les alertes sont manquées hebdomadairement et 21 % ont déclaré qu'elles sont manquées quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 60 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 91 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 43 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 96 % des personnes interrogées se déclarent **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 54 % d'entre elles déclarent que plus de 40 % des alertes sont de faible priorité.

53 %

reçoivent plus de 500 alertes de sécurité cloud par jour

52 %

indiquent que la fatigue des alertes a contribué à la rotation du personnel

91 %

font confiance à la précision de leurs outils de sécurité ?

Principales conclusions
France

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 61 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 40 % déclarent que plus de 40 % de leurs alertes sont des faux positifs et 43 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 45 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement professionnel, la rotation du personnel et des frictions internes :** 76 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel et 79 % ont déclaré que la fatigue des alertes a créé des frictions internes.
- **Des alertes critiques sont manquées, souvent sur une base quotidienne ou hebdomadaire :** parmi les 77 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 40 % ont déclaré que les alertes sont manquées hebdomadairement et 26 % quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 60 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 99 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 40 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 97 % des personnes interrogées se déclarent **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 43 % déclarent que plus de 40 % des alertes sont de faible priorité.

61 %

reçoivent plus de 500 alertes de sécurité cloud par jour

76 %

indiquent que la fatigue des alertes a contribué à la rotation du personnel

99 %

font confiance à la précision de leurs outils de sécurité ?

Principales conclusions

Allemagne

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 54 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 41 % déclarent que plus de 40 % de leurs alertes sont des faux positifs et 48 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 50 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement professionnel, la rotation du personnel et des frictions internes :** 65 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel et 60 % ont déclaré que la fatigue des alertes a créé des frictions internes.
- **Des alertes critiques sont manquées, souvent quotidiennement ou hebdomadairement :** parmi les 56 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 54 % ont déclaré que les alertes sont manquées hebdomadairement et 19 % ont déclaré qu'elles sont manquées quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 43 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 95 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 41 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 96 % des personnes interrogées se déclarent **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 48 % d'entre elles déclarent que plus de 40 % des alertes sont de faible priorité.

54 %

reçoivent plus de 500 alertes de sécurité cloud par jour

65 %

indiquent que la fatigue des alertes a contribué à la rotation du personnel

95 %

font confiance à la précision de leurs outils de sécurité ?

Principales conclusions

Australie

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 61 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 36 % disent que plus de 40 % de leurs alertes sont des faux positifs et 42 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 56 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement professionnel, la rotation du personnel et des frictions internes :** 62 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel et 57 % ont déclaré que la fatigue des alertes a créé des frictions internes.
- **Des alertes critiques sont manquées, souvent sur une base quotidienne ou hebdomadaire :** parmi les 56 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 39 % ont déclaré que les alertes sont manquées hebdomadairement et 20 % ont déclaré qu'elles sont manquées quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 61 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 94 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 36 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 97 % des personnes interrogées se déclarent **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 40 % d'entre elles déclarent que plus de 40 % des alertes sont de faible priorité.

61 %

reçoivent plus de 500 alertes de sécurité cloud par jour

62 %

indiquent que la fatigue des alertes a contribué à la rotation du personnel

94 %

font confiance à la précision de leurs outils de sécurité ?

Principales conclusions

Service financier mondial

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 71 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 42 % déclarent que plus de 40 % de leurs alertes sont des faux positifs et 51 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 63 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement professionnel, la rotation du personnel et des frictions internes :** 65 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel et 58 % déclarent que la fatigue des alertes a créé des frictions internes.
- **Des alertes critiques sont manquées, souvent sur une base quotidienne ou hebdomadaire :** parmi les 61 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 35 % ont déclaré que les alertes sont manquées sur une hebdomadairement, et 25 % ont déclaré qu'elles sont manquées quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 58 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 91 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 42 % déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 94 % des personnes interrogées se déclarent **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 51 % déclarent que plus de 40 % des alertes sont de faible priorité.

71 %

reçoivent plus de 500 alertes de sécurité cloud par jour

65 %

indiquent que la fatigue des alertes a contribué à la rotation du personnel

91 %

font confiance à la précision de leurs outils de sécurité ?

Principales conclusions

Soins de santé mondiaux

La fatigue des alertes en chiffres :

- **Les équipes chargées de la sécurité sont inondées d'alertes de sécurité cloud :** 53 % des personnes interrogées reçoivent plus de 500 alertes de sécurité informatique par jour.
- **Un grand nombre d'alertes sont inexactes ou inutiles :** 32 % déclarent que plus de 40 % de leurs alertes sont des faux positifs et 45 % déclarent que plus de 40 % des alertes sont de faible priorité.
- **L'examen et la hiérarchisation des alertes constituent une tâche importante :** 48 % passent plus de 20 % de leur journée à examiner les alertes et à décider lesquelles doivent être traitées en premier.

La fatigue des alertes entraîne la rotation du personnel et des alertes critiques manquées :

- **La fatigue des alertes entraîne l'épuisement professionnel, la rotation du personnel et des frictions internes :** 58 % des personnes interrogées déclarent que la fatigue des alertes a contribué à la rotation du personnel, et 58 % ont déclaré que la fatigue des alertes a créé des frictions internes.
- **Des alertes critiques sont manquées, souvent quotidiennement ou hebdomadairement :** parmi les 48 % de personnes interrogées qui déclarent que des alertes critiques sont manquées, 41 % ont déclaré que les alertes sont manquées hebdomadairement, et 34 % ont déclaré qu'elles sont manquées quotidiennement.

La barre des outils de sécurité est-elle placée trop bas ?

- 53 % ont **5 outils de sécurité sur le cloud public ou plus**.
- 97 % des personnes interrogées déclarent **faire confiance ou pleinement confiance à la précision** de leurs outils de sécurité, même si 32 % d'entre elles déclarent que plus de 40 % de leurs alertes sont des faux positifs.
- 97 % des personnes interrogées disent qu'elles sont **satisfaites ou très satisfaites de la façon dont leurs outils de sécurité hiérarchisent les risques**, même si 45 % d'entre elles déclarent que plus de 40 % des alertes sont de faible priorité.

53 %

reçoivent plus de 500 alertes de sécurité cloud par jour

58 %

indiquent que la fatigue des alertes a contribué à la rotation du personnel

97 %

font confiance à la précision de leurs outils de sécurité ?

À propos d'Orca Security

Orca Security fournit une sécurité et une conformité instantanées pour AWS, Azure et GCP, sans les lacunes en matière de couverture, la fatigue des alertes et les coûts de fonctionnement des agents ou des sidecars. Simplifiez les opérations de sécurité du cloud avec une seule plateforme CNAPP pour la protection des charges de travail et des données, la gestion de la posture de sécurité du cloud (CSPM), la gestion des vulnérabilités et la conformité.

Orca Security hiérarchise les risques en fonction de la gravité du problème de sécurité, de son accessibilité et de son impact commercial. Cela vous aide à vous concentrer sur les alertes critiques qui comptent le plus. Les innovateurs mondiaux, dont Databricks, Autodesk, NCR, Gannett et Robinhood, font confiance à Orca Security.

Connectez votre premier compte en quelques minutes : https://orca.security ou faites l'évaluation des risques cloud gratuite.