SÉCURITÉ DU CLOUD HYBRIDE :
perception vs. réalité

Une enquête mondiale menée auprès de plus de 1 000 responsables de l'informatique et de la sécurité révèle que la perception que beaucoup ont de la sécurité et de la visibilité de leur cloud hybride ne correspond pas à la réalité. L'étude révèle également que l'évolution de la législation est désormais une préoccupation majeure des RSSI, ce qui montre que l'observabilité avancée est plus importante que jamais.

PERCEPTION vs. RÉALITÉ

94% des répondants dans le monde **affirment que leurs outils et processus de sécurité leur fournissent une visibilité complète et des informations** sur leur infrastructure IT.

50% sont confiants ou tout à fait **confiants quant à la sécurité** de l'ensemble de leur infrastructure IT, depuis leurssites jusqu'au cloud.

96% des répondants reconnaissent que **la sécurité du cloud dépend d'une meilleure visibilité sur l'ensemble des données en mouvement.**

97% reconnaissent qu'ils peuvent **collaborer au sein de leur organisation IT** lorsqu'il s'agit de détecter les vulnérabilités et d'y répondre.

SEULEMENT 30% **ont la visibilité sur les données chiffrées,** et un tiers des RSSI ne sont pas sûrs de savoir comment leurs données sensibles sont sécurisées.

SEULEMENT 10% **n'ont pas subi de violation de données au cours** des 18 derniers mois.

PLUS DE 30% **des violations de données n'ont pas été détectées** par les outils de sécurité / d'observabilité.

PLUS DE 16% des entreprises ne pratiquent **toujours pas la responsabilité collective**, les SecOps étant souvent considérés comme les seuls responsables de la sécurité.

Il existe une certaine forme de naïveté vis-à-vis des dangers liés au manque de visibilité

Bien qu'elles soient convaincues de disposer d'une parfaite visibilité, les équipes IT et de sécurité admettent l'existence d'un certain nombre de lacunes en termes de visibilité au sein de leur infrastructure IT.

Les considèrent-elles comme des menaces ?

26%
Plus d'un quart (26 %) des répondants dans le monde s'inquiètent de ne pas disposer des outils / de la visibilité nécessaires pour sécuriser leur organisation.

52%
n'ont pas de visibilité sur les données circulant latéralement - autrement dit sur le trafic est-ouest.

35%
ont une visibilité limitée sur le trafic entre conteneurs.

Les angles morts insoupçonnés
pouvant être exploités sont la principale préoccupation des répondants **(56 %)**.

La législation
(34 %) est une importante source de stress, la loi européenne sur la cyber-résilience étant la plus problématique à l'échelle mondiale.

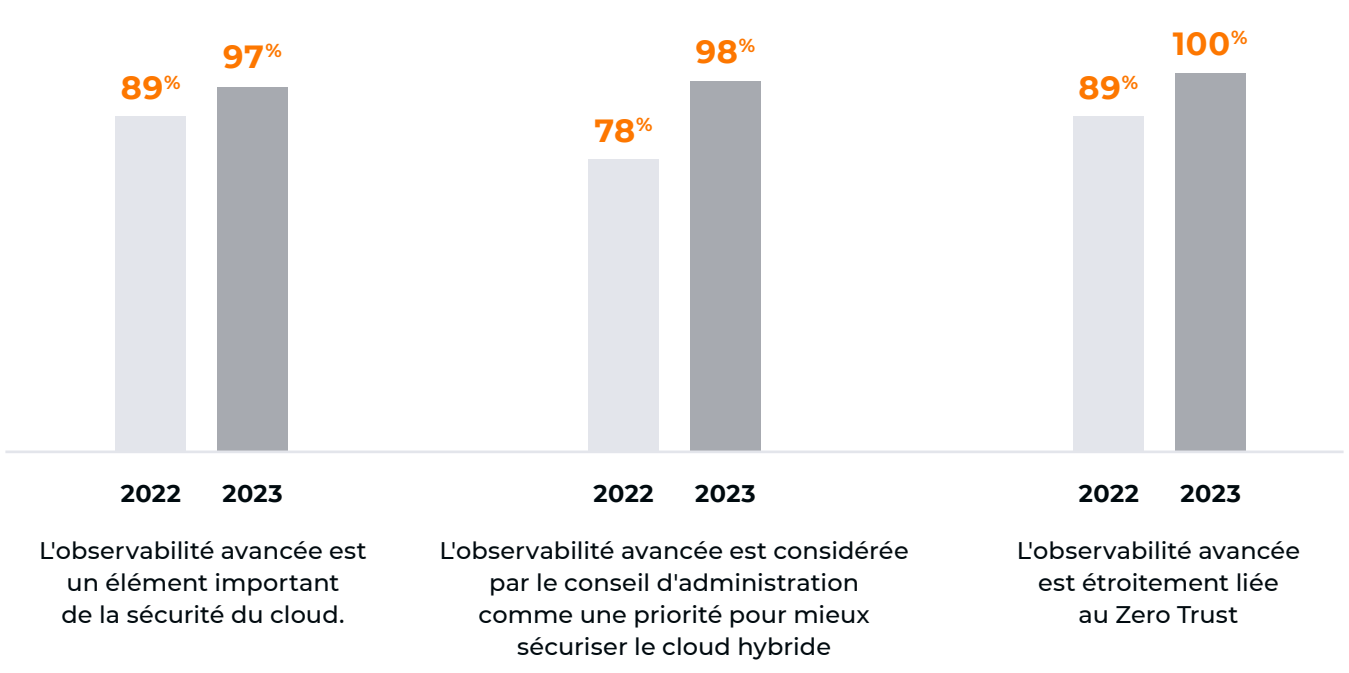
La complexité des attaques
est une plus grande crainte **(32 %)** pour les RSSI que le manque d'investissements dans la cybersécurité **(14 %)**.

Les angles morts et la législation empêchent les RSSI de bien dormir

Les préoccupations concernant la pénurie attendue de compétences et les investissements sont peu présentes dans l'esprit des responsables IT et de sécurité en 2023. **Seuls 19 % d'entre eux affirment qu'une formation efficace du personnel en matière de sécurité est un facteur essentiel** pour gagner en confiance dans la sécurité de l'infrastructure IT.

OBSERVABILITÉ AVANCÉE : de plus en plus partie intégrante de la sécurité du cloud et du Zero Trust

L'importance de l'observabilité avancée ne cesse de se confirmer chez les décideurs de l'IT et sécurité de 2022 à 2023.



Découvrez l'ensemble des résultats de votre région dans le rapport complet : gigamon.com/enquete-cloud-securite

Collecte des données : du 19 avril au 2 mai 2023
Répondants : 1 020 DSI / RSSI / Directeurs de la technologie et autres professionnels des réseaux et du cloud
Régions : États-Unis, Royaume-Uni, France, Allemagne, Singapour, Australie

Gigamon®