Kiteworks

# Analyse 2024 des communications de contenu sensible pour la Sécurité et la Défense : les tendances en matière de sécurité et de conformité

## CHIFFRES CLÉS

| | | |
|---|---|---|
| **Outils de communication utilisés** | 16% | Plus de 7 |
| | 27% | 6 |
| | 14% | 5 |
| | 15% | 4 |
| | 20% | 3 |
| | 6% | 2 |
| | 1% | 1 |
| | 1% | Ne sait pas |
| **Échange de contenu sensible avec des tiers** | 7% | Plus de 5 000 |
| | 26% | 2 500 à 4 999 |
| | 39% | 1 000 à 2 499 |
| | 18% | 500 à 999 |
| | 10% | Moins de 499 |
| **Types de données les plus préoccupantes (Top 3)** | 53% | Documents financiers |
| | 50% | LLMs de GenAI |
| | 50% | PI |
| | 41% | Échanges juridiques |
| | 36% | PII |
| | 34% | PHI |
| | 26% | CUI et FCI |
| | 12% | Fusions & Acquisitions |
| **Top 2 des priorités sur la confidentialité et la conformité réglémentaire** | 41% | HIPAA |
| | 38% | Lois des États américains |
| | 38% | CMMC |
| | 32% | RGPD |
| | 28% | Exigences SEC |
| | 18% | PCI DSS |
| | 6% | Lois propres à chaque pays |
| **Top 2 des certificats de sécurité les plus importants** | 50% | ISO 27001, 27017, 27018 |
| | 44% | NIST 800-171/CMMC 2.0 |
| | 38% | FedRAMP Moderate |
| | 35% | IRAP (Australie) |
| | 22% | SOC 2 Type II |
| | 11% | Directive NIS 2 |
| **Nombre de piratages des communications de contenu sensible** | 3% | Plus de 10 |
| | 39% | 7 à 9 |
| | 26% | 4 à 6 |
| | 20% | 2 à 3 |
| | 7% | 1 |
| | 5% | Ne sait pas |

Le rapport Kiteworks 2024 sur la confidentialité et la conformité des communications de contenu sensible fournit une analyse détaillée des problématiques et des pratiques dans différents secteurs d'activité, et notamment pour la Sécurité et la Défense. Ce brief reprend les principales conclusions du rapport concernant ces secteurs ; outils utilisés pour échanger des données sensibles, problèmes de cybersécurité, risques dans les échanges avec des tiers, menaces spécifiques et conséquences sur la conformité règlementaire.

## Gestion de tous les outils de communication de contenu sensible

57 % des acteurs de la sécurité et de la défense utilisent au moins cinq outils de communication pour envoyer et partager des contenus sensibles, ce qui est plus que la moyenne de l'ensemble de la cohorte (53 %). 41 % d'entre eux déclarent pouvoir suivre et contrôler les données sensibles envoyées et partagées en interne, et 39 % seulement lorsqu'elles sont échangées en externe. Ce résultat est nettement moins bon que celui des autres secteurs d'activité : 51 % et 43 % respectivement. Des chiffres inquiétants pour les agences du DoD.

Les répondants ont cité la prévention des litiges longs et coûteux et les fuites de propriété intellectuelle et secrets d'entreprise comme leurs deux préoccupations majeures (à 57 % et 50 %). Le premier est légèrement supérieur à l'ensemble de la cohorte (51 %), tandis que le second est inférieur (56 %).

## Évaluer le risque tiers pour les contenus sensibles

La gestion des risques liés aux tiers est une préoccupation majeure pour toutes les organisations. Les acteurs de la Sécurité et de la Défense échangent des données sensibles avec un nombre d'interlocuteurs sensiblement identique à celui des autres secteurs d'activité (33 % avec plus de 2 500 tiers). Et comme la plupart des autres secteurs, ils ont des difficultés à suivre et à contrôler les informations sensibles qui quittent une application. Seuls 10 % d'entre eux affirment être en mesure de le faire dans 100 % des cas, tandis que 37 % déclarent pouvoir le faire dans maximum 50 % des cas.

## Évaluer le niveau de conformité pour les contenus sensibles

83 % des acteurs de la Sécurité et de la Défense ont indiqué que leur système de management de la conformité des communications sensibles nécessitait des améliorations importantes (22%) ou quelques améliorations (60%). Ce chiffre est légèrement supérieur à celui de l'ensemble des répondants : 88 %.

Étonnamment, l'HIPAA arrive en tête des priorités des entreprises du secteur de la sécurité et de la défense (41 %). La CMMC 2.0 arrive en deuxième avec 38 %, à égalité avec les lois propres à chaque État américain. Quant aux lois propres à chaque pays, elles sont les moins citées (6 %). D'après d'autres études, la majorité des prestataires de services de sécurité et de défense ne sont pas prêts à appliquer la CMMC. Or elle va devenir obligatoire très prochainement ; le fait qu'elle n'ait pas été citée en premier a de quoi inquiéter.

Pour ce qui est des certifications de sécurité, 50 % des entreprises de sécurité et de défense ont cité les normes ISO 27001, 27017 et 27018 parmi leurs deux priorités. 44 % ont cité le NIST 800-171/CMMC comme leur norme de certification/validation de sécurité n°1. FedRAMP Moderate arrive en troisième position (38 %), et la directive NIS 2 a été la moins citée (11 %).

## Évaluer les risques liés à la sécurité des contenus sensibles

Même tendance que pour la conformité règlementaire : les entreprises du secteur de la sécurité et de la défense ont besoin d'améliorer la sécurité de leurs communications sensibles de manière plus ou moins importante, et ce plus souvent que dans les autres secteurs. Les outils de sécurité avancés (chiffrement, authentification multifactorielle, suivi et contrôle de la gouvernance) ne sont utilisés que par 55 % des entreprises en interne (contre 59 % pour l'ensemble de la cohorte) et 51 % en externe (contre 59 % pour l'ensemble de la cohorte). Ces chiffres sont signe d'une lacune majeure à corriger.

## Évaluer le coût de la sécurité et de la conformité

Les organisations de la sécurité et de la défense sont souvent la cible des cybercriminels et des États voyous, en raison du contenu sensible et confidentiel envoyé et partagé. Le nombre de violations de données signalées l'année dernière est alarmant : 42 % des personnes interrogées ont déclaré que leur organisation avait subi sept violations de données ou plus (contre 32 % pour l'ensemble de la cohorte).

En termes de coûts, l'enquête a révélé que les entreprises de sécurité et de défense étaient très exposées. Plus de la moitié d'entre elles (53 %) ont admis avoir dépensé plus de 3 millions de dollars par an en litiges liés aux violations de données (contre 45 % pour l'ensemble des répondants).

## Connaissance et classification des types de données

Près de la moitié (48 %) des entreprises de sécurité et de défense déclarent étiqueter et classer plus des trois quarts des données non structurées, et 28 % déclarent étiqueter et classer plus de la moitié. Ces pourcentages sont similaires aux chiffres mondiaux, où 48 % des entreprises déclarent étiqueter et classer les trois quarts ou plus de leurs données non structurées.

Lorsqu'on leur demande quelle proportion de leurs données non structurées a besoin d'être étiquetée et classée, 27 % répondent 60 % ou plus et 47 % répondent que 40 à 60 % des données non structurées devraient l'être.

# Urgence absolue à protéger les contenus sensibles dans le secteur de la Sécurité et de la Défense

Le rapport Kiteworks 2024 souligne l'importance de la gestion des risques et de la conformité pour les communications de contenu sensible des professionnels de la sécurité et de la défense.

Ils sont 53 % à se soucier prioritairement des documents financiers et 50 % à se soucier des LLM d'IA générative et de la propriété intellectuelle (à égalité). Les organisations de la sécurité et de la défense sont aussi nombreuses que celles des secteurs de l'énergie et des services publics à citer les LLMs de GenAI à 50 %.

En pratique, les répondants évoluant dans la sécurité et la défense passent beaucoup de temps à compiler les journaux d'audit générés par les nombreux outils de communication de contenus sensibles. Près de 3 sur 10 déclarent y consacrer au moins 2 000 heures par an, et 38 % entre 1 500 et 2 000 heures.

Accéder au rapport complet