Kiteworks

NOTE DE CONFORMITÉ

# Conformité à la loi sur la cyberrésilience de l'UE

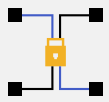
## Kiteworks garantit une gestion sécurisée de tous les produits contenant des éléments numériques

La loi sur la cyberrésilience établit des règles de cybersécurité pour les produits contenant des éléments numériques commercialisés au sein de l'UE. Elle vise à améliorer la sécurité des produits matériels et logiciels tout au long de leur cycle de vie, et à permettre aux utilisateurs de prendre en compte ce critère au moment de l'achat. Le texte impose aux fabricants des règles de sécurité pour la conception et le développement des produits, ainsi que pour la gestion des vulnérabilités. Il fixe également des procédures d'évaluation règlementaire, en particulier pour les produits critiques fabriqués par des sous-traitants. Enfin, le CRA oblige les fabricants à communiquer sur les garanties de sécurité et les mises à jour. À cette fin, l'UE va mettre en place des mécanismes de surveillance du marché et d'application de la règlementation. Le règlement s'applique à tous les produits matériels et logiciels connectables, à quelques exceptions près. Toute infraction est passible de sanctions financières, avec des amendes pouvant aller jusqu'à 15 millions d'euros ou 2,5 % du chiffre d'affaires annuel mondial, le montant le plus élevé des deux étant retenu. Au-delà de l'aspect économique, les organisations risquent des restrictions d'accès au marché, une atteinte à leur image de marque et une surveillance renforcée de la part des autorités règlementaires. Autrement dit, de se retrouver en difficulté et de perdre leur avantage concurrentiel sur le marché européen. De cette façon, l'UE cherche à créer un cadre cohérent pour éviter la prolifération des règles nationales, tout en renforçant la sécurité et la confiance des utilisateurs dans les produits numériques.

### Évaluer et maîtriser les risques grâce à une plateforme « Secure by Design », ou sécurisée dès sa conception

Le CRA exige une évaluation des risques cybernétiques pour les produits contenant des éléments numériques tout au long de leur cycle de vie ; identification des vulnérabilités, adoption de mesures de sécurité, mises à jour continues et respect des principes du « Secure-by-design ». Kiteworks facilite ce travail grâce à son cycle de développement de logiciels qui comprend des tests internes et externes, des vérifications de code, des tests d'intrusion et des programmes de primes à la détection de bugs. Les entreprises ont la responsabilité de vérifier la conformité de leurs fournisseurs, de maintenir à jour la nomenclature des logiciels et de rechercher les vulnérabilités à chaque étape de leur développement. Kiteworks applique les meilleures pratiques du secteur : normes OWASP, accès accordés selon le principe du moindre privilège et protection renforcée des systèmes d'information. Une équipe de sécurité dédiée gère l'analyse et la

## Avantages de la solution



**Cycle de développement sécurisé**

**Tests en continu**

**Principes du moindre privilège par défaut**

**Journalisation en temps réel**

**Mises à jour accessibles en un clic**

**Tableau de bord RSSI**

correction des vulnérabilités pour anticiper les risques tout au long du cycle de vie du produit. Kiteworks assure ainsi la prévention des menaces et l'amélioration continue de la sécurité de ses produits, pour proposer à ses clients des solutions robustes et conformes au CRA et autres règlementations de cybersécurité.

## Signaler les incidents et corriger les vulnérabilités grâce à la journalisation en temps réel et à des mises à jour efficaces

La gestion des vulnérabilités et le signalement des incidents sont des contrôles essentiels. Le CRA impose des exigences strictes de reporting et de signalement des incidents ou des vulnérabilités activement exploitées, auprès de l'Agence de l'Union européenne pour la cybersécurité, et ce dans les 24 heures suivant leur découverte. Grâce à la journalisation exhaustive en temps réel et à l'intégration SIEM, Kiteworks accélère la détection et la réponse rapide en cas d'incident. La plateforme applique des tests de vulnérabilité en continu : tests d'intrusion automatisés et manuels, programmes de primes à la détection de bugs et audits externes. La plateforme intègre des mises à jour accessibles en un clic qui garantissent un déploiement rapide des correctifs dans les environnements en cluster. Ces mesures de sécurité simplifient la tâche des organisations pour limiter les risques de cybersécurité conformément aux exigences de la loi sur la cyberrésilience. Les journaux d'audit consolidés dans la plateforme consignent toutes les activités liées à la sécurité, et facilitent l'analyse des incidents et le reporting. En outre, la nomenclature logicielle de Kiteworks améliore la transparence et favorise la correction des vulnérabilités au niveau des composants et des dépendances du produit.

## Des journaux d'audit immuables pour une documentation et une transparence totales

Dans le cadre du CRA, les fabricants sont tenus de fournir une documentation technique complète et des instructions d'utilisation claires. Ils doivent apposer sur leurs produits le marquage CE indiquant la conformité avec le CRA. Et surtout, garder une trace du respect de ces obligations et de tous les problèmes rencontrés. Cet historique pourrait être consulté par les autorités en cas de besoin. Ces nouvelles mesures responsabilisent les industriels et permettent de contrôler les pratiques de cybersécurité. Par ailleurs, Kiteworks fournit une description détaillée des logiciels accessible depuis la console d'administration par les administrateurs autorisés. Conformément aux normes industrielles (comme NIST CSF), Kiteworks centralise la gestion des accès, des ressources et des journaux d'audit selon des procédures strictes. C'est un outil de supervision efficace, avec des journaux d'audit détaillés, une intégration SIEM et un tableau de bord RSSI. Kiteworks conserve précieusement toute la documentation relative au cycle de développement de ses logiciels et met à disposition la documentation technique et les consignes d'utilisation nécessaires. En plus de simplifier la préparation des audits, cela responsabilise et favorise la coopération avec les autorités. En fournissant des informations claires et accessibles, Kiteworks aide les organisations à se conformer aux exigences de transparence du CRA et à le prouver.

Kiteworks fournit une plateforme sécurisée conforme aux exigences de la loi européenne sur la cyberrésilience, qui assure la gestion complète de la sécurité des produits comportant des éléments numériques. Avec un cycle de développement logiciel sécurisé, des tests en continu et des mesures de sécurité proactives, Kiteworks garantit l'évaluation et la maîtrise des risques à tout moment. La journalisation en temps réel, l'intégration SIEM et le système de mise à jour performant de la plateforme simplifient le signalement rapide des incidents et la correction des vulnérabilités. Enfin, la nomenclature logicielle accessible et les journaux d'audit détaillés facilitent le travail de documentation et de transparence. L'ensemble de ces caractéristiques permet aux entreprises de répondre aux exigences des normes industrielles telles que le NIST CSF et le CRA ; principes « Secure-by-design », signalement des incidents et traçabilité totale. Avec Kiteworks, les entreprises peuvent se concentrer sur leur activité sans craindre les évolutions règlementaires en matière de cybersécurité. Les risques maîtrisés, elles conservent leur avantage concurrentiel sur le marché de l'UE. La plateforme protège les professionnels des sanctions et des atteintes à l'image de marque que causeraient des problèmes de non-conformité.