KAIA-OR · FICHE TECHNIQUE · ENTREPRISE

Seulement les événements qui touchent vos sites, chacun avec son degré de corroboration.

Les risques, les incidents de sécurité, les perturbations et les cyberévénements reliés à vos sites, à vos logiciels et à vos fournisseurs dans une image commune, chacun avec sa gravité, son niveau de confiance, sa source et le motif de la correspondance.

IDENTIFIANT DU DOCUMENT	DS-ENTERPRISE
VERSION	1.0
DATE	3 novembre 2026
PUBLIC	Les personnes qui dirigent la sécurité, et leurs équipes des opérations de sécurité, des risques liés aux voyages, de la protection de la haute direction et de la cybersécurité

Pour qui

Les responsables de la sécurité qui dirigent un centre des opérations de sécurité ou une fonction de risques liés aux voyages, de protection de la haute direction ou de cybersécurité, et qui ont besoin d'une image unique sur laquelle agir et à citer dans leurs breffages. KAIA-OR Entreprise donne à l'organisation une image commune de ses sites, de ses logiciels et de ses fournisseurs, tandis que chaque personne garde son propre KAIA-OR.

L'enjeu

- **Trop de bruit.** Les alertes générales épuisent les équipes, et l'événement qui touche réellement un site passe facilement inaperçu.
- **Personne ne peut agir sur la foi d'un signalement non confirmé.** Sans vue claire de la gravité, du niveau de confiance et de la corroboration, les équipes ne peuvent ni informer la direction ni décider.
- **Des équipes cloisonnées.** Les équipes de la sécurité physique, des voyages, de la protection de la haute direction et de la cybersécurité travaillent avec des outils distincts, si bien que les liens entre les événements se perdent.

> Dans un sondage mené en 2026 auprès de spécialistes des risques, les cyberincidents arrivaient au premier rang des risques mondiaux pour la cinquième année consécutive, avec 42 % des réponses; l'interruption des activités se classait au troisième rang, et les catastrophes naturelles au cinquième, avec 21 %.[1]

Ce que vous obtenez

Physique, cyber et chaîne d'approvisionnement dans une même image

Les risques, les incidents et les perturbations qui touchent vos sites; les violations de données d'envergure et les vulnérabilités nouvellement exploitées qui touchent les logiciels que vous utilisez; et les fournisseurs qui y sont exposés.

Un niveau de confiance que vous pouvez présenter à la direction

Chaque événement indique sa gravité, son niveau de confiance, sa source et son état de corroboration, et les signalements non confirmés sont indiqués comme tels.

© Kaia Technologies, Inc.

Personnel à l’étranger : ce qui a changé, et un second regard

Chaque personne en déplacement voit quels événements touchent son voyage et ce qui a changé dans les conseils officiels aux voyageurs, et obtient un second regard sur les messages et les liens suspects. L’organisation voit ses sites, et non l’endroit où se trouvent ses membres.

Vos événements dans vos propres outils

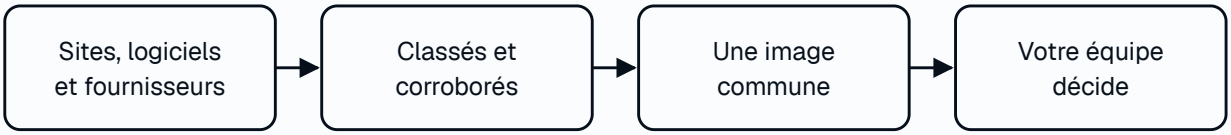
Transmettez les événements et leurs données probantes à vos propres outils au moyen d’une API documentée et de crochets Web (webhooks).

L’IA soumise aux données probantes

Les réponses sont vérifiées au regard des données probantes et les citent. Les résultats produits par le modèle n’accordent aucune autorité, et les agents d’exploration agissent uniquement dans les limites que vous fixez et avec votre autorisation.

© Kaia Technologies, Inc.

Une journée avec KAIA-OR



Une image commune pour l'organisation; chaque personne garde son propre KAIA-OR.

1. L'équipe de sécurité ajoute les bureaux, les centres de données et les fournisseurs clés, ainsi que les logiciels dont dépend l'organisation.
2. Lorsqu'une vulnérabilité nouvellement exploitée touche un logiciel qu'utilise l'organisation, elle s'affiche dans la même image que les sites, avec les fournisseurs qui y sont exposés.
3. Lorsqu'un signalement de risque ou d'incident concerne un site, l'équipe voit sa gravité, son niveau de confiance, sa source et son état de corroboration. Les signalements non confirmés sont indiqués comme tels.
4. L'équipe informe la direction à partir de cette image et transmet l'événement à ses propres outils au moyen de l'API documentée.
5. Une personne en déplacement à l'étranger voit ce qui a changé dans les conseils officiels aux voyageurs pour sa destination et obtient un second regard sur un message suspect.

Confidentialité et contrôle

- L'organisation voit ses sites, et non l'endroit où se trouvent ses membres. La position exacte de chaque personne en déplacement reste sur son propre appareil.
- Les rôles gèrent l'adhésion, pas les personnes. L'adhésion ne donne jamais accès aux messages, aux appareils, à la position ni aux lieux enregistrés d'un autre membre. Ces limites de l'adhésion, ainsi que l'isolement entre les organisations, sont appliqués dans la couche applicative.
- Rien n'est transmis à l'IA infonuagique sans votre accord préalable.
- Les membres se connectent au moyen du fournisseur d'identité de l'organisation. Les personnes ayant le rôle Propriétaire ou Administrateur téléchargent les revues des accès datées et voient qui a changé quoi, et quand.

© Kaia Technologies, Inc.

Adapté aux entreprises et aux gouvernements

KAIA-OR s'intègre aux outils d'identité, de sécurité et de gouvernance qu'une organisation utilise déjà.

Fonctionnalité	Ce que cela signifie pour vous
Authentification unique et gestion des comptes	Les membres se connectent au moyen de votre fournisseur d'identité, et SCIM 2.0 crée et supprime leurs comptes au fil des changements dans votre annuaire.
Clés d'accès et connexion par application d'authentification	Connectez-vous avec une clé d'accès, ou avec votre mot de passe et une application d'authentification comme deuxième étape. Les codes de connexion ne sont jamais envoyés par texto.
Des rôles selon le moindre privilège	Définissez vos propres rôles en plus des rôles Propriétaire, Administrateur et Membre, chacun doté uniquement des autorisations dont il a besoin.
Exportation du journal d'audit	Exportez le journal d'audit de l'organisation vers vos propres outils de sécurité, en plus des revues des accès datées que vous conservez déjà.
Choix de la résidence des données	Choisissez la région où sont conservées les données de votre organisation.
L'IA infonuagique sous votre contrôle	Désactivez les fonctions d'IA infonuagique pour votre espace de travail. Ce contrôle ne fait que restreindre : il n'active jamais l'IA infonuagique pour un membre et ne passe jamais outre au choix d'un membre.
Vos outils, au moyen de l'API	Transmettez les événements et les données probantes à vos propres systèmes au moyen de l'API et de crochets Web (webhooks).

Plateformes et langues

Plateformes	iOS, iPadOS, macOS, les téléphones Android, Android TV, Windows et le Web.
Langues	Anglais, français (Canada), turc et hébreu, avec une mise en page entièrement de droite à gauche en hébreu.

Un même compte fonctionne sur toutes les plateformes, avec les mêmes fonctionnalités et les mêmes règles de confidentialité.

Forfait

KAIA-OR Entreprise. Consultez la page Forfaits du site Web de KAIA-OR.

© Kaia Technologies, Inc.

Demander un accès anticipé

> L’adhésion se fait sur invitation. Demandez un accès anticipé sur le site Web de KAIA-OR et choisissez le forfait Entreprise, ou utilisez la page Nous joindre du site Web de KAIA-OR.

Sources

1. Allianz Commercial, Allianz Risk Barometer 2026, janvier 2026. Contexte du marché uniquement.

© Kaia Technologies, Inc.

DS-ENTERPRISE · Version 1.0 · 3 novembre 2026

La disponibilité des fonctionnalités dépend du forfait et du déploiement. Les fonctionnalités décrites correspondent à la portée engagée du produit KAIA-OR.