KAIA-OR · LIVRE BLANC · INTELLIGENCE SUR LES ÉVÉNEMENTS

Du volume à la pertinence

Une intelligence de sécurité axée sur la pertinence : comment KAIA-OR détermine quels risques, incidents, perturbations et cyberévénements méritent votre attention, à quel point il en est sûr, et pourquoi chacun correspond.

IDENTIFIANT DU DOCUMENT	WP-1
VERSION	1.0
DATE	3 novembre 2026
PUBLIC	Responsables de la sécurité, des risques, des voyages et des opérations en entreprise et dans l'administration publique; équipes sans fonction de sécurité; personnes chargées de l'évaluation technique; particuliers et familles avertis

Table des matières

1. Sommaire 3

2. Du volume à la pertinence 4
   1. Le problème de la surcharge 4
   2. Ce que signifie la pertinence 4
   3. Comment un événement vous parvient 5

3. Corroboration, niveau de confiance et motif 6
   1. Ce que vous apprend chaque événement 6
   2. La corroboration n'est pas le niveau de confiance 6
   3. Montrer le motif, et ce qui a changé 7

4. Pertinence et confidentialité, ensemble 8
   1. La mise en correspondance sur l'appareil 8
   2. Des alertes personnelles à une image commune 8

5. L'IA soumise aux données probantes 10
   1. Comprendre les événements 10
   2. Des réponses vérifiées au regard des données probantes 10
   3. L'autorité reste entre les mains des personnes 11

6. Portée, en toute transparence, et liste de vérification pour l'acquisition 12

7. Ce que cela signifie pour vous 14
   1. Glossaire 14

© Kaia Technologies, Inc.

Sommaire

La plupart des personnes et des organisations ne manquent pas d'information sur les événements qui les menacent. Ce qui leur manque, c'est un moyen de savoir quels événements les concernent, à quel point on peut en être sûr, et quoi faire ensuite. Les alertes arrivent par de nombreux canaux, dans de nombreux formats et avec peu de contexte. Le résultat est bien connu : des alarmes générales que l'on apprend à ignorer, des équipes de sécurité qui passent leur journée à trier des signalements au lieu de prendre des décisions, et l'événement qui comptait, remarqué trop tard.

KAIA-OR repose sur une autre prémisse, que nous appelons l'**intelligence de sécurité axée sur la pertinence** : une image unique et explicable des risques physiques, cyber et liés aux voyages, adaptée à ce dont chaque personne et chaque organisation est responsable. Ce que vous signalez à KAIA-OR comme important pour vous (vos lieux, vos voyages, vos sites, vos logiciels et vos fournisseurs) détermine ce que vous voyez. Les risques naturels, les incidents de sécurité, les perturbations des infrastructures et les cyberévénements proviennent de sources officielles et faisant autorité, et sont corroborés auprès de sources indépendantes. Chaque événement est classé par catégorie et décrit par sa gravité, son lieu, sa période et son niveau de confiance, ainsi que par son état de corroboration. Il est ensuite mis en correspondance avec ce qui vous concerne, sur votre appareil, et affiché avec le motif de la correspondance.

Quatre engagements guident la conception :

- **La pertinence.** Vous voyez les événements qui touchent vos propres lieux, voyages, sites, logiciels et fournisseurs, et non un flux non filtré.
- **L'explication.** Chaque événement indique le motif de la correspondance et son degré de corroboration, et les conseils aux voyageurs que vous suivez indiquent ce qui a changé à chaque nouvelle révision.
- **Les données probantes avant les réponses.** L'assistant, Hey KAIA, répond par la voix ou par écrit. Ses réponses sont vérifiées au regard des données probantes et les citent, et les résultats produits par le modèle n'accordent aucune autorité.
- **Les personnes décident.** KAIA-OR suggère une prochaine étape. Il n'agit au nom de personne sans son autorisation.

Ce livre blanc explique chacun de ces engagements sur le plan conceptuel. Il décrit des principes, l'architecture conceptuelle et les résultats. Ce n'est pas un guide de mise en œuvre : il ne nomme aucune source et ne publie ni les mécanismes internes ni le modèle de données sous-jacent. Il se termine par une liste de vérification qui permet d'évaluer la pertinence d'une solution, quel que soit le fournisseur envisagé.

> **À PROPOS DE CE LIVRE BLANC**
> Ce livre blanc décrit la conception et la portée engagée du produit KAIA-OR. La disponibilité des fonctionnalités dépend du forfait et du déploiement. Les statistiques sont citées à titre de contexte du marché, avec leur émetteur et leur date dans la section Sources, et ne mesurent jamais l'effet d'un produit, quel qu'il soit.

© Kaia Technologies, Inc.

1. Du volume à la pertinence

Le problème de la surcharge

L'information de sécurité n'a jamais été aussi abondante. Les organismes publics, les exploitants, les milieux de la recherche et la presse publient une multitude de rapports, et toute organisation d'une certaine taille reçoit en plus des bulletins, des avis aux voyageurs et des rapports internes. La difficulté n'est plus l'accès, mais l'attention. Trois schémas reviennent, qu'il s'agisse d'une personne, d'une famille, d'une petite équipe ou d'une grande organisation.

- **Des alarmes générales.** Une alerte qui porte sur une région, un secteur ou une technologie n'indique pas si elle touche un bureau précis, un voyage précis ou un produit précis. Lorsque la plupart des alertes ne s'appliquent pas, les gens cessent de les lire, y compris celles qui s'appliquent.
- **La fragmentation.** L'information physique, l'information sur les voyages et l'information cyber se trouvent dans des outils différents, gérés par des personnes différentes. Personne ne fait le lien entre une inondation régionale, une vague de fraudes qui l'exploite et le voyage d'un collègue dans la ville touchée.
- **L'incertitude.** Les premiers signalements sont souvent partiels, et certains sont faux. Sans indication claire du degré de corroboration d'un signalement, les personnes qui décident agissent sur la foi de rumeurs ou attendent une certitude qui arrive trop tard.

Les équipes de sécurité finissent par trier et éliminer les doublons au lieu d'exercer leur jugement. Les équipes sans fonction de sécurité, les particuliers et les familles l'apprennent tout simplement trop tard, par les personnes qu'ils servent, par des proches ou par les nouvelles.

L'ampleur des risques en jeu est bien documentée. 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] Les risques physiques et cyber figurent côte à côte sur la même liste, mais ils sont rarement présentés au même endroit.

Ce que signifie la pertinence

Dans KAIA-OR, la pertinence est définie par la personne ou l'organisation, et non par le produit. Vous indiquez à KAIA-OR ce qui compte, et cela détermine ce que vous voyez.

CE QUE VOUS INDIQUEZ À KAIA-OR, ET CE QUI REND UN ÉVÉNEMENT PERTINENT

Vous ajoutez	Par exemple	Un événement est pertinent lorsque
Lieux	Le domicile, le travail, une ville où vivent des proches	Son lieu et sa période touchent un lieu que vous avez enregistré
Voyages	Une destination et des dates de voyage	Il touche votre destination ou votre itinéraire pendant vos dates, ou les conseils pour cette destination changent
Sites	Un bureau, un commerce, un entrepôt, une usine, un poste	Il touche un site dont votre organisation est responsable

© Kaia Technologies, Inc.

Vous ajoutez	Par exemple	Un événement est pertinent lorsque
Logiciels	Les produits et les services sur lesquels votre organisation s'appuie	Il porte sur une violation de données d'envergure ou sur une vulnérabilité nouvellement exploitée dans un logiciel que vous utilisez
Fournisseurs	Les organisations dont vous dépendez	Un fournisseur est exposé à un événement critique ou à une vulnérabilité nouvellement exploitée

Les événements qui ne touchent aucun de ces éléments ne se disputent pas votre attention. Mettre la pertinence au premier plan ne veut pas dire offrir moins d'information. Cela signifie que ce que vous voyez est choisi selon des critères que vous fixez, avec le motif affiché. La même approche sert une personne et une organisation; le chapitre 3 explique comment les deux coexistent.

Comment un événement vous parvient

Sur le plan conceptuel, chaque événement suit les mêmes six étapes, de ce qui vous importe jusqu'à la décision que vous prenez.



Figure 1. Les six étapes conceptuelles. Les éléments personnels restent sur l'appareil de la personne; les sites d'une organisation vont dans son image commune. La figure est conceptuelle et ne décrit pas une mise en œuvre.

© Kaia Technologies, Inc.

2. Corroboration, niveau de confiance et motif

Ce que vous apprend chaque événement

Dans KAIA-OR, un événement est plus qu'un titre. Chacun comporte un petit ensemble d'attributs, présentés en langage clair, pour que l'on puisse en juger sans ouvrir un rapport distinct.

LES ATTRIBUTS AFFICHÉS AVEC CHAQUE ÉVÉNEMENT

Attribut	La question à laquelle il répond
Catégorie	De quel type d'événement s'agit-il : un risque naturel, un incident de sécurité, une perturbation des infrastructures ou un cyberévénement?
Gravité	Quel est son degré de gravité, décrit dans les mêmes termes simples d'une catégorie à l'autre?
Lieu	Où se produit-il, ou quelle zone touche-t-il?
Période	Quand a-t-il commencé, et pendant quelle période compte-t-il?
Niveau de confiance	À quel point KAIA-OR est-il sûr de l'événement tel qu'il est décrit?
Source	D'où vient le signalement?
État de corroboration	Des sources indépendantes signalent-elles le même événement? Les signalements sans corroboration indépendante sont indiqués comme non confirmés.
Motif de la correspondance	Lesquels de vos lieux, voyages, sites, logiciels ou fournisseurs touche-t-il?

La corroboration n'est pas le niveau de confiance

- **La corroboration** consiste à savoir si des sources indépendantes signalent le même événement. Elle exprime l'accord entre les sources.
- **Le niveau de confiance** exprime à quel point KAIA-OR est sûr de ce qui est décrit : le lieu, le moment et la gravité, compte tenu de ce que l'on sait à ce moment-là.

Les deux peuvent diverger. Un signalement clairement décrit provenant d'une seule source faisant autorité peut être précis, tout en attendant une deuxième source. Plusieurs signalements sommaires peuvent s'accorder sur le fait que quelque chose s'est produit, sans en préciser l'ampleur. Afficher les deux permet de distinguer « s'est probablement produit, détails incertains » de « clairement décrit, corroboration en attente », et d'informer la direction en conséquence.

Les premiers signalements comptent; KAIA-OR ne les retient donc pas jusqu'à ce que leurs détails soient établis. Il les affiche avec leur mention, et cette mention change à mesure que la corroboration arrive, ou n'arrive pas. La corroboration constitue une donnée probante, et non une preuve, et KAIA-OR la présente ainsi : un événement est décrit comme corroboré ou non confirmé, jamais comme un fait établi.

© Kaia Technologies, Inc.

> **CE QUE NOUS PUBLIONS, ET CE QUE NOUS NE PUBLIONS PAS**
>
> Nous publions la signification de chaque attribut, et non les mécanismes internes qui le produisent. Publier ces mécanismes aiderait quiconque souhaite fabriquer un signalement qui semble corroboré, sans aider pour autant à juger un événement donné.

Montrer le motif, et ce qui a changé

Chaque événement de votre vue indique le motif de la correspondance : le lieu enregistré dont il est proche, le voyage dont il recoupe la destination et les dates, le site qu'il touche, le logiciel qu'il concerne ou le fournisseur en cause. Cette explication remplit trois fonctions.

- **La confiance.** Vous pouvez vérifier le raisonnement au lieu d'accepter un verdict les yeux fermés.
- **La correction.** Si une correspondance est erronée parce qu'un lieu, un voyage ou un site n'est plus à jour, vous pouvez corriger l'information saisie, plutôt que d'apprendre à ignorer le produit.
- **Le breffage.** Une personne responsable de la sécurité peut transmettre un événement à la direction avec son motif, sa gravité, son niveau de confiance et son état de corroboration.

Une grande partie de l'information de sécurité ne porte pas sur un nouvel événement, mais sur un changement. Les conseils pour une destination sont révisés. Un incident s'intensifie ou s'apaise. Une vulnérabilité jusque-là théorique est signalée comme exploitée. Pour les conseils aux voyageurs que vous suivez, chaque nouvelle révision indique les dates de publication précédente et nouvelle ainsi que les champs modifiés, pour que personne n'ait à relire un long avis afin de trouver la ligne qui a changé. Les explications s'affichent en anglais, en français (Canada), en turc ou en hébreu, avec une mise en page entièrement de droite à gauche en hébreu.

© Kaia Technologies, Inc.

3. Pertinence et confidentialité, ensemble

La mise en correspondance sur l'appareil

Pour un usage personnel, la comparaison entre les événements entrants et les lieux et voyages enregistrés d'une personne s'effectue sur l'appareil de cette personne. Les lieux et les voyages restent sur l'appareil. La position exacte aussi. Lorsqu'une personne demande ce qui se passe à proximité, KAIA-OR utilise une seule position, prise au moment même, pour cette vérification, et l'efface lorsqu'elle arrête. Les notifications ne nomment jamais le lieu ni l'événement : un écran verrouillé ne révèle donc ni l'endroit où se trouve une personne ni ce qui lui importe.

C'est un choix de conception, et c'est là que pertinence et confidentialité se renforcent mutuellement. Un service qui met les événements en correspondance de façon centralisée doit savoir où les personnes qui l'utilisent vivent, travaillent et voyagent, et tenir cette information à jour. Un service qui effectue la mise en correspondance sur l'appareil n'en a pas besoin. Plus KAIA-OR établit des correspondances précises pour une personne, moins il a besoin d'en savoir sur elle de façon centralisée. Pertinence et confidentialité vont dans le même sens, au lieu d'être sacrifiées l'une à l'autre.

Le même principe s'applique à l'assistant. Hey KAIA fonctionne d'abord sur l'appareil. Rien n'est transmis à un service d'IA infonuagique sans l'accord préalable de la personne, et pour les organismes gouvernementaux, l'IA infonuagique est désactivée au départ.

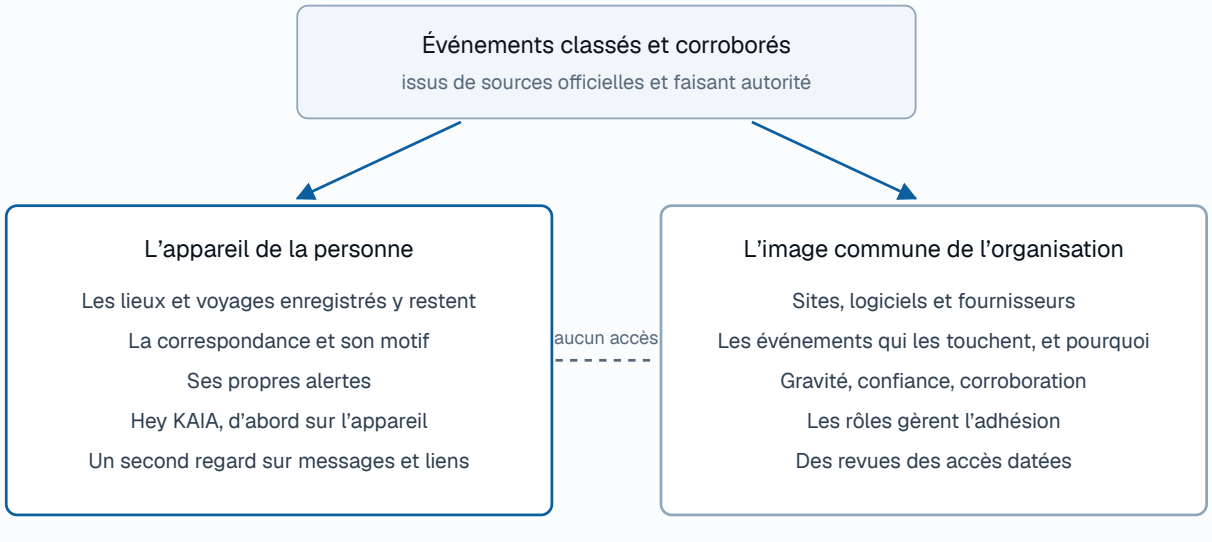


Figure 2. Deux cases bien distinctes : l'appareil et l'organisation. Être membre ne donne pas accès. L'organisation voit ses sites, et non l'endroit où se trouvent ses membres.

Des alertes personnelles à une image commune

KAIA-OR est un seul produit, d'une personne à un organisme gouvernemental. Les forfaits Individuel, Famille, Équipe, Entreprise et Gouvernement partagent la même intelligence sur les événements et les mêmes explications. Dans une organisation, deux images coexistent.

© Kaia Technologies, Inc.

- **L’image commune** réunit les sites, les logiciels et les fournisseurs de l’organisation, ainsi que les événements qui les touchent, à l’intention des personnes responsables. Un événement qui touche un commerce, un bureau ou un entrepôt s’affiche sur le site concerné, avec sa gravité, son état de corroboration et le motif de la correspondance. Les événements survenus de l’autre côté d’une frontière ou en mer qui touchent un site y figurent aussi.
- **Le KAIA-OR propre à chaque membre** réunit ses propres lieux et voyages, ses propres alertes et son propre second regard sur les messages et les liens. Chaque personne en déplacement voit ce qui a changé dans les conseils officiels aux voyageurs pour son propre voyage.

Les rôles gèrent l’adhésion, pas les personnes. L’organisation voit ses sites, et non l’endroit où se trouvent ses membres. L’adhésion ne donne jamais accès aux messages, aux appareils, à la position ni aux lieux enregistrés d’un autre membre. Les accès sont consignés : les invitations sont à usage unique et liées à un compte, et les revues des accès sont datées.

Dans toute votre chaîne d’approvisionnement. Les fournisseurs exposés à des événements critiques ou à des vulnérabilités nouvellement exploitées figurent dans la même image que vos sites, de sorte qu’un événement physique chez un fournisseur et un cyberévénement dans un logiciel partagé sont vus ensemble.

Dans vos propres outils. Les événements peuvent parvenir aux outils existants de l’organisation au moyen d’une API documentée et de crochets Web (webhooks). L’intelligence axée sur la pertinence rejoint alors les flux de travail que l’équipe utilise déjà, au lieu d’ajouter un écran de plus.

© Kaia Technologies, Inc.

4. L'IA soumise aux données probantes

KAIA-OR utilise l'intelligence artificielle à trois endroits : pour comprendre les événements, pour les expliquer et pour répondre aux questions au moyen de l'assistant. Dans chaque cas, une seule règle s'applique : l'IA informe, et les personnes décident. Ce chapitre emploie quelques termes techniques de catégorie, chacun accompagné de ce qu'il signifie pour vous.

Comprendre les événements

Les événements sont décrits dans de nombreux vocabulaires et de nombreuses langues. KAIA-OR les ramène à un vocabulaire commun : une **ontologie** des risques, des incidents, des perturbations, des cyberévénements, des lieux, des organisations, des logiciels et des fournisseurs, organisée sous forme de **graphe de connaissances**. Pour vous, le résultat est la cohérence. Un même type d'événement est reconnu quels que soient les mots qu'emploie une source : une inondation reste une inondation et un fournisseur reste un fournisseur, d'où que vienne le signalement.

Le **raisonnement sémantique** détermine ce qu'est un événement et ce qu'il touche. Un raisonnement sur la façon dont les situations sont liées, se déroulent et évoluent dans le temps relie une panne à la tempête qui l'a causée, ou une vague de fraudes à l'événement qu'elle exploite, et suit un incident à mesure qu'il s'intensifie ou s'apaise. Le résultat : moins d'alertes en double et un compte rendu plus clair de ce qui a changé.

Des réponses vérifiées au regard des données probantes

Hey KAIA répond par la voix ou par écrit, en anglais, en français, en turc ou en hébreu, et fonctionne d'abord sur l'appareil. Un **modèle de langage** excelle à lire et à rédiger en langage naturel, mais reconnaît mal ses propres erreurs. KAIA-OR l'associe donc à des vérifications symboliques, une approche appelée **raisonnement neurosymbolique**. Le modèle de langage propose une réponse. Cette réponse est vérifiée au regard des données probantes conservées dans KAIA-OR avant que vous la voyiez, et elle cite ces données probantes. Lorsque les données probantes n'appuient pas une affirmation, l'assistant indique ce qu'il ne peut pas établir au lieu de combler le vide. Le résultat : un assistant dont vous pouvez vérifier les réponses.

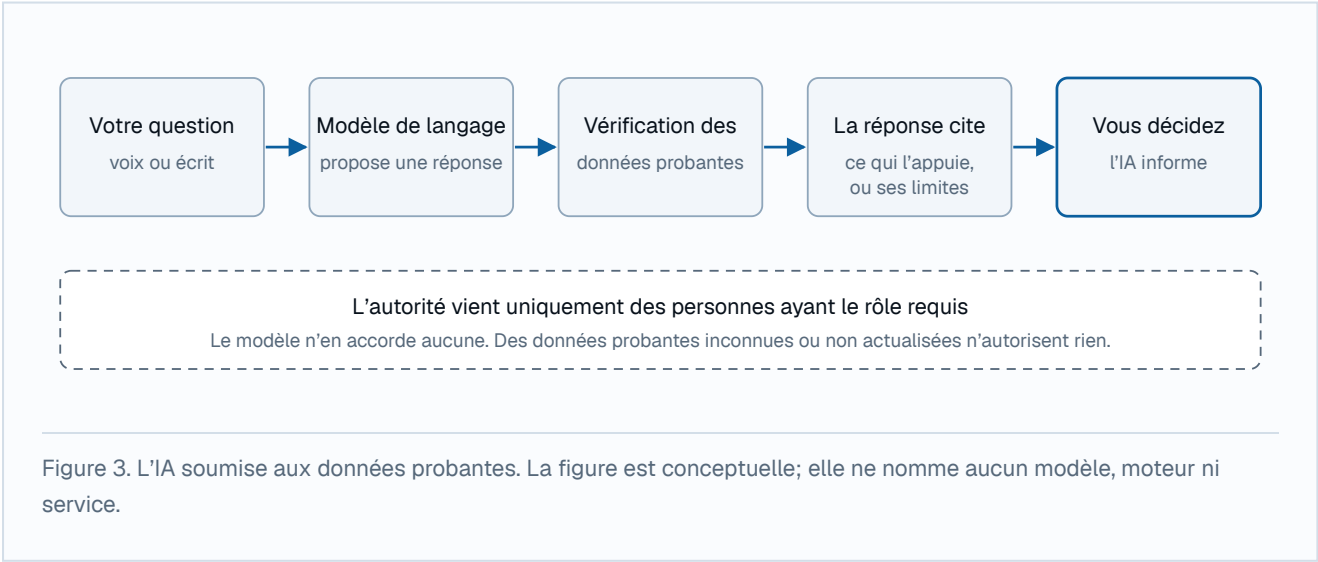


Figure 3. L'IA soumise aux données probantes. La figure est conceptuelle; elle ne nomme aucun modèle, moteur ni service.

© Kaia Technologies, Inc.

En matière de risques, l'assistant relaie les consignes de l'émetteur lui-même. Il ne rédige jamais ses propres consignes de sécurité. Pour les messages et les liens, il suggère une prochaine étape, par exemple confirmer par un canal auquel vous faites déjà confiance, et la décision vous revient.

L'autorité reste entre les mains des personnes

Les résultats produits par le modèle n'accordent aucune autorité. Rien de ce que produit un modèle ne peut approuver une action, modifier une autorisation ni élargir ce qu'un agent peut faire. L'autorité vient uniquement des personnes qui ont le rôle requis, au moyen des contrôles du produit lui-même. Cette règle tient même lorsque le contenu que lit un modèle a été conçu pour le manipuler. L'assistant est conçu pour résister aux instructions dissimulées dans le contenu qu'il lit et aux tentatives d'ingénierie sociale qui visent l'IA elle-même.

Des agents d'exploration encadrés. Les agents d'exploration accomplissent des tâches définies, dans les limites que fixe la personne ou l'organisation, par exemple repérer les événements nouvellement signalés qui touchent les logiciels ou les fournisseurs d'une organisation. Ils agissent uniquement avec votre autorisation. Des données probantes inconnues ou non actualisées n'autorisent jamais une action. Aucun agent ne prend de mesure destructrice, n'envoie de message ni n'effectue d'achat au nom de quiconque sans autorisation explicite.

Ces règles permettent à l'IA d'être utile en sécurité sans devenir une source de risque de plus. Le modèle aide les gens à lire plus vite et à voir des liens. Il ne devient jamais celui qui décide.

© Kaia Technologies, Inc.

5. Portée, en toute transparence, et liste de vérification pour l'acquisition

L'intelligence axée sur la pertinence n'est utile que dans la mesure où elle est franche sur ses limites. KAIA-OR est conçu en fonction de quatre d'entre elles.

- **Une couverture vaste, mais limitée.** Aucun ensemble de sources ne décrit le monde entier, ni ne publie à la même vitesse partout. KAIA-OR s'appuie sur des sources officielles et faisant autorité partout dans le monde, et corrobore les signalements auprès de sources indépendantes. Il ne prétend pas voir tout ce qui se passe, et l'absence d'alertes ne démontre pas qu'il ne s'est rien passé. Le moment où un événement s'affiche dépend du moment où les sources le publient et de sa corroboration; KAIA-OR ne fait donc aucune promesse quant aux délais.
- **Lorsqu'une vérification ne peut pas se prononcer, elle le dit.** Certaines questions ne peuvent pas être tranchées à partir des données probantes disponibles. KAIA-OR indique alors clairement qu'il ne peut pas se prononcer et suggère une façon de le savoir, plutôt que d'offrir un verdict qu'il ne peut pas étayer.
- **Les consignes des émetteurs en matière de risques.** Pour les risques naturels et les événements touchant la sécurité publique, KAIA-OR relaie les consignes de l'émetteur. Il ne rédige pas ses propres consignes de sécurité et ne conclut pas à l'absence de danger pour un lieu ou un voyage.
- **Les décisions restent entre les mains des personnes.** KAIA-OR informe et suggère des prochaines étapes. La responsabilité des décisions revient à la personne ou à l'organisation.

Les questions ci-dessous peuvent être posées à n'importe quel fournisseur, y compris nous. Elles permettent de distinguer la pertinence du volume.

LISTE DE VÉRIFICATION POUR ÉVALUER LA PERTINENCE AVANT L'ACQUISITION

Question à poser	Une réponse solide
Qui décide de ce qui est pertinent : le fournisseur ou vous?	Vous définissez vos lieux, vos voyages, vos sites, vos logiciels et vos fournisseurs, et vous voyez ce qui les touche.
Chaque événement indique-t-il le motif de la correspondance?	Oui, en langage clair, à côté de l'événement, dans la langue de la personne qui le lit.
La corroboration et le niveau de confiance sont-ils affichés séparément?	Oui. L'accord entre des sources indépendantes est distingué de la certitude quant aux détails.
Où la mise en correspondance a-t-elle lieu, et qu'apprend le fournisseur sur l'endroit où se trouvent les gens?	La mise en correspondance personnelle s'effectue sur l'appareil de la personne, et la position exacte y reste.
Les réponses de l'IA sont-elles vérifiées au regard des données probantes, et les citent-elles?	Oui, avant que la personne ne les voie, et l'assistant indique ce qu'il ne peut pas établir.
Les résultats du modèle peuvent-ils modifier des autorisations ou déclencher des actions?	Non. L'autorité vient uniquement des personnes qui ont le rôle requis, et les agents n'agissent qu'avec une autorisation.

© Kaia Technologies, Inc.

Question à poser	Une réponse solide
La vue de l'organisation s'arrête-t-elle à ses sites?	Oui. Elle ne s'étend ni à l'endroit où se trouvent ses membres, ni à leurs messages, ni à leurs appareils.
Comment le fournisseur décrit-il sa couverture?	Franchement : vaste, avec ses limites énoncées, et sans promesse quant à la rapidité.

© Kaia Technologies, Inc.

Ce que cela signifie pour vous

Particuliers et familles. Vous voyez les risques, les incidents, les perturbations et les cyberévénements qui touchent les lieux que vous enregistrez et les voyages que vous prévoyez, chacun avec le motif de la correspondance et son degré de corroboration. Vos lieux et votre position exacte restent sur votre appareil. Demandez à Hey KAIA ce qu'un événement signifie pour vous, par la voix ou par écrit, dans votre langue.

Équipes sans fonction de sécurité. Sans équipe d'opérations de sécurité, vous voyez les événements qui touchent vos sites, avec leur gravité, leur corroboration et le motif de la correspondance, ainsi qu'une prochaine étape suggérée. Chaque membre garde ses propres alertes et son propre second regard.

Équipes de sécurité, de gestion des voyages et de cybersécurité des entreprises. L'exposition physique, cyber et de la chaîne d'approvisionnement figure dans une même image commune, reliée à vos sites, à vos logiciels et à vos fournisseurs. Chaque événement indique sa gravité, son niveau de confiance, sa source et son état de corroboration, et les événements peuvent parvenir à vos propres outils au moyen de l'API et de crochets Web (webhooks).

Organismes gouvernementaux. Vos sites et vos missions figurent dans une même image dont votre équipe peut se servir pour ses breffages, chaque événement avec sa source, son état de corroboration et son niveau de confiance. Pour les organismes gouvernementaux, l'IA infonuagique est désactivée au départ. Les résultats produits par le modèle n'accordent aucune autorité, et les agents d'exploration agissent uniquement avec votre autorisation. Vos responsables décident.

Pour évaluer KAIA-OR, demandez un accès anticipé sur le site Web de KAIA-OR. Les équipes d'entreprise et des organismes gouvernementaux peuvent aussi choisir Nous joindre sur le site Web de KAIA-OR.

Glossaire

Terme	Sens dans ce livre blanc
État de corroboration	Indique si des sources indépendantes signalent le même événement. Les signalements sans corroboration indépendante sont indiqués comme non confirmés.
Ontologie	Un vocabulaire commun des types d'événements, de lieux et d'actifs que comprend KAIA-OR, pour qu'un même événement soit reconnu quels que soient les mots qui le décrivent.
Graphe de connaissances	La forme connectée sous laquelle ce vocabulaire et les relations entre les événements, les lieux et les actifs sont conservés, pour que des événements liés puissent être reliés entre eux.
Modèle de langage	Une IA qui lit et rédige en langage naturel. Dans KAIA-OR, le modèle propose; il ne décide jamais.
Raisonnement neurosymbolique	L'association d'un modèle de langage et de vérifications symboliques, pour que les réponses soient vérifiées au regard des données probantes avant que quiconque les voie.

© Kaia Technologies, Inc.

Sources

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

© Kaia Technologies, Inc.

WP-1 · 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.