KAIA-OR · NOTE PAR CAS D'UTILISATION

Risque numérique et renseignement sur les cybermenaces

Voyez les cyberévénements qui touchent les logiciels qu'utilise votre organisation, dans la même image que vos sites, et offrez à votre personnel un second regard sur les messages et les liens.

IDENTIFIANT DU DOCUMENT	UCB-04-DIGITAL-RISK-AND-CYBER-THREAT-INTELLIGENCE
VERSION	1.0
DATE	3 novembre 2026
PUBLIC	Responsables de la sécurité et des TI des équipes, des entreprises et des organismes gouvernementaux

En bref

Pour qui	Les organisations qui dépendent de logiciels qu'elles n'ont pas conçus, et dont le personnel reçoit des messages d'hameçonnage, des liens suspects et des fichiers douteux.
Résultat	Seulement les violations de données d'envergure et les vulnérabilités nouvellement exploitées qui touchent les logiciels que vous utilisez, chacune avec sa gravité, son niveau de confiance et son état de corroboration, à côté des événements physiques qui touchent vos sites, ainsi qu'un second regard pour votre personnel.
Forfait	KAIA-OR Équipe, Entreprise ou Gouvernement

L'enjeu

Les équipes de la sécurité et des TI reçoivent plus de signalements de vulnérabilités et de violations de données qu'elles ne peuvent en lire. Les plus utiles sont ceux qui touchent les logiciels que leur organisation utilise réellement, et pour les trouver, il faut parcourir de nombreux signalements qui ne la concernent pas.

Parallèlement, des personnes de toute l'organisation reçoivent des messages d'hameçonnage, des liens piégés et des fichiers suspects. Les petites équipes n'ont pas de personnel de sécurité à consulter, et les grandes équipes ne peuvent pas examiner chaque message que reçoit leur personnel.

Les cyberévénements sont généralement suivis dans un outil et les événements physiques dans un autre : l'équipe responsable d'un bureau voit une tempête à un endroit et, ailleurs, une vulnérabilité dans les logiciels qu'utilise ce bureau, sans que rien ne relie les deux.

© Kaia Technologies, Inc.

Ce que KAIA-OR change

Les cyberévénements qui touchent vos logiciels

Les violations de données d'envergure et les vulnérabilités nouvellement exploitées qui touchent les logiciels que vous utilisez s'affichent comme des événements, chacun avec sa gravité, son niveau de confiance, sa source et son état de corroboration, ainsi que le motif de la correspondance.

Physique et cyber dans une même image

Les cyberévénements figurent dans la même image commune que les risques, les incidents et les perturbations qui touchent vos sites, pour que les personnes responsables d'un site voient les deux.

Un second regard pour votre personnel

Les membres du personnel collent un message suspect ou vérifient un lien sans l'ouvrir. Ils voient ce qui semble anormal, les cas où la vérification ne peut pas se prononcer et une prochaine étape suggérée, par exemple confirmer par un canal auquel ils font déjà confiance. Les vérifications reconnaissent les signaux d'alerte en anglais, en français, en turc et en hébreu.

Indicateurs de risque liés aux fichiers et aux logiciels espions

Pour les fichiers et les appareils, KAIA-OR présente les indicateurs de risque qui méritent un examen plus attentif, sans verdict.

Dans vos propres outils

Les événements parviennent aux outils que votre équipe utilise déjà au moyen de l'API et de crochets Web (webhooks).

Des réponses que vous pouvez vérifier

Demandez à Hey KAIA ce qu'un événement signifie pour les logiciels que vous utilisez. Les réponses citent leurs données probantes et sont vérifiées au regard de celles-ci. 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.

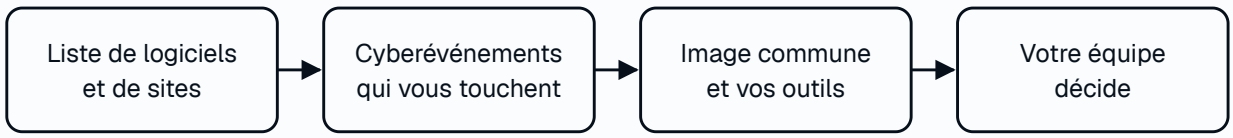
Ce que vous voyez

Élément	Ce qu'il présente
Un cyberévénement	La catégorie, la gravité, la période, le niveau de confiance, la source et l'état de corroboration, les logiciels qu'il touche et le motif de la correspondance.
L'image commune	Les cyberévénements à côté des événements physiques qui touchent vos sites.

© Kaia Technologies, Inc.

Élément	Ce qu'il présente
Une vérification de message ou de lien	Les signaux d'alerte reconnus et une prochaine étape suggérée, sans que le lien soit ouvert.
Une vérification de fichier ou de logiciel espion	Les indicateurs de risque qui méritent un examen plus attentif, sans verdict.

Fonctionnement



Des cyberévénements reliés aux logiciels que vous indiquez, dans la même image que vos sites.

1. Une personne responsable de la sécurité indique les principaux logiciels qu'utilise l'organisation et ajoute ses bureaux comme sites.
2. Lorsqu'une vulnérabilité nouvellement exploitée touche l'un de ces produits, elle s'affiche comme un événement dans l'image commune, avec sa gravité, son niveau de confiance, son état de corroboration et le motif de la correspondance.
3. Selon le forfait, l'événement parvient aussi aux propres outils de l'équipe au moyen de l'API et de crochets Web (webhooks), pour qu'il atteigne les personnes qui traitent déjà ce type de travail.
4. Lorsqu'un membre du personnel reçoit un message contenant un lien dont il doute, il le colle. Le lien n'est pas ouvert, et il voit ce qui semble anormal et une prochaine étape suggérée.
5. La personne responsable de la sécurité demande à Hey KAIA ce que la vulnérabilité signifie pour l'organisation. La réponse cite ses données probantes, et la décision sur la marche à suivre revient à l'équipe.

© Kaia Technologies, Inc.

Confidentialité et contrôle

- Les messages et les liens que chaque personne vérifie restent 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 liées à 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. Pour les organismes gouvernementaux, l'IA infonuagique est désactivée au départ.

Limites, en toute transparence

- KAIA-OR n'est pas un antivirus. Il informe, et il ne modifie, ne supprime ni ne corrige rien de lui-même dans vos systèmes.
- Les résultats relatifs aux fichiers et aux logiciels espions sont des indicateurs de risque, pas des verdicts. KAIA-OR ne conclut pas à l'absence de danger pour un fichier, un lien ou un appareil.
- Les cyberévénements sont reliés aux logiciels que vous indiquez. La couverture dépend de ce que publient les sources officielles et faisant autorité, et les signalements qui ne peuvent pas être corroborés sont indiqués comme non confirmés.

Forfaits et cas d'utilisation connexes

Le risque numérique fait partie des forfaits Équipe, Entreprise et Gouvernement. L'accès à l'API dépend du forfait; consultez la page Forfaits du site Web de KAIA-OR. KAIA-OR fonctionne sur iOS, iPadOS, macOS, les téléphones Android, Android TV, Windows et le Web, en anglais, en français (Canada), en turc et en hébreu. Un même compte fonctionne sur toutes les plateformes, avec les mêmes fonctionnalités et les mêmes règles de confidentialité.

Cas d'utilisation connexes

- Vérification des fraudes et de l'hameçonnage
- Chaîne d'approvisionnement
- Services financiers

© 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 Équipe, Entreprise ou Gouvernement. Les équipes d’entreprise et du secteur public peuvent aussi utiliser la page Nous joindre du site Web de KAIA-OR.

© Kaia Technologies, Inc.

UCB-04-DIGITAL-RISK-AND-CYBER-THREAT-INTELLIGENCE · 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.