KAIA-OR · USE-CASE BRIEF

Digital risk and cyber threat intelligence

See the cyber events that touch the software your organization uses, in the same picture as your sites, and give your people a second look at messages and links.

DOCUMENT ID	UCB-04-DIGITAL-RISK-AND-CYBER-THREAT-INTELLIGENCE
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Security and IT leads in teams, enterprises and government organizations

At a glance

Who it is for	Organizations that depend on software they did not build, and whose people receive phishing messages, suspicious links and files.
Outcome	Only the major breaches and newly exploited vulnerabilities that touch the software you use, each with severity, confidence and corroboration status, next to the physical events that touch your sites, plus a second look for your people.
Package	KAIA-OR Team, Enterprise or Government

The challenge

Security and IT teams receive more vulnerability and breach reports than they can read. The useful ones are those that touch the software their organization actually uses, and finding them means reading through many that do not.

At the same time, people across the organization receive phishing messages, malicious links and suspicious files. Small teams have no security staff to ask, and larger teams cannot review each message their people receive.

Cyber events usually live in one tool and physical events in another, so the team responsible for an office sees a storm in one place and a vulnerability in the software that office runs in another, with nothing connecting them.

© Kaia Technologies, Inc.

What changes with KAIA-OR

Cyber events that touch your software

Major breaches and newly exploited vulnerabilities that touch the software you use appear as events, each with its severity, confidence, source and corroboration status, and the reason it matched.

Physical and cyber in one picture

Cyber events sit in the same shared picture as the hazards, incidents and disruptions that touch your sites, so the people responsible for a site see both.

A second look for your people

Staff paste a suspicious message or check a link while it stays unopened. They see what looks wrong, when the check can't tell, and a suggested next step, such as confirming through a channel they already trust. The checks recognize warning signs in English, French, Turkish and Hebrew.

File and spyware risk indicators

For files and devices, KAIA-OR shows risk indicators worth a closer look, with no verdict.

Into your own tools

Events flow into the tools your team already uses through the API and webhooks.

Answers you can check

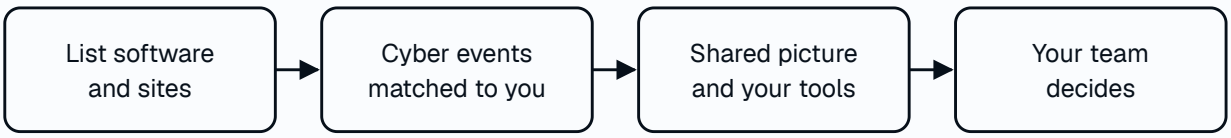
Ask Hey KAIA what an event means for the software you use. Answers cite their evidence and are checked against it. Model output grants no authority, and scanning agents act only within the limits you set and with your authorization.

What you see

Item	What it shows
A cyber event	Category, severity, time window, confidence, source and corroboration status, the software it touches and the reason it matched.
The shared picture	Cyber events next to the physical events that touch your sites.
A message or link check	The warning signs recognized and a suggested next step, with the link left unopened.
A file or spyware check	Risk indicators worth a closer look, with no verdict.

© Kaia Technologies, Inc.

How it works



Cyber events matched to the software you list, in the same picture as your sites.

1. A security lead lists the main software the organization uses and adds its offices as sites.
2. When a newly exploited vulnerability touches one of those products, it appears as an event in the shared picture, with its severity, confidence, corroboration status and the reason it matched.
3. Depending on the package, the event also flows into the team's own tools through the API and webhooks, so it reaches the people who already handle such work.
4. When a member of staff receives a message with a link they are unsure about, they paste it in. The link stays unopened, and they see what looks wrong and a suggested next step.
5. The security lead asks Hey KAIA what the vulnerability means for the organization. The answer cites its evidence, and the decision about what to do stays with the team.

© Kaia Technologies, Inc.

Privacy and control

- The messages and links each person checks stay on their own device.
- Roles manage membership, not people. Membership never grants access to another member's messages, devices, location or saved places.
- These membership boundaries, and the isolation between organizations, are enforced at the application layer.
- Nothing goes to cloud AI unless you agree first. Government organizations start with cloud AI off.

Honest boundaries

- KAIA-OR is not antivirus. It informs, and it does not change, remove or patch anything on your systems on its own.
- File and spyware results are risk indicators, not verdicts. KAIA-OR does not issue an all-clear for a file, a link or a device.
- Cyber events are matched to the software you list. Coverage depends on what official and authoritative sources publish, and reports that cannot be corroborated are labelled as unconfirmed.

Editions and related use cases

Digital risk is part of the Team, Enterprise and Government packages. API access depends on the package; see Packages on the KAIA-OR website. KAIA-OR runs on iOS, iPadOS, macOS, Android phones, Android TV, Windows and the web, in English, French (Canada), Turkish and Hebrew. One account works on every platform, with the same features and the same privacy rules.

Related use cases

- Scam and phishing checks
- Supply chain
- Financial services

© Kaia Technologies, Inc.

Request early access

> Membership is by invitation. Request early access on the KAIA-OR website and choose Team, Enterprise or Government. Enterprise and government teams can also choose Contact us on the KAIA-OR website.

© Kaia Technologies, Inc.

UCB-04-DIGITAL-RISK-AND-CYBER-THREAT-INTELLIGENCE · Version 1.0 · 3 November 2026

Capability availability depends on the edition and deployment. Capabilities are described as the committed KAIA-OR product scope.