KAIA-OR · USE-CASE BRIEF

Supply chain

See which suppliers are exposed to critical events and newly exploited vulnerabilities, in the same picture as your own sites.

DOCUMENT ID	UCB-09-SUPPLY-CHAIN
VERSION	1.0
DATE	3 November 2026
AUDIENCE	Supply-chain, procurement, resilience and security teams

At a glance

Who it is for	Organizations that depend on suppliers and facilities in many countries, and on software that suppliers provide.
Outcome	Supplier exposure to hazards, incidents, disruptions and newly exploited vulnerabilities, shown next to your own sites and sent into your own tools.
Package	KAIA-OR Team, Enterprise or Government

The challenge

When a storm closes a port, unrest shuts a district or a vulnerability is exploited in widely used software, the first question is which of your suppliers is affected. The answer usually takes days of calls and spreadsheets, because physical events and cyber events are followed in separate tools by separate teams.

Supply chains span suppliers and facilities across many countries, and teams need evidence they can act on: which supplier, which event, how well it is corroborated, and why it matters to you. They also need that evidence in the systems they already use, without a heavy integration project.

© Kaia Technologies, Inc.

What changes with KAIA-OR

Supplier exposure in one picture

Hazards, security incidents and infrastructure disruptions that touch a supplier's facilities appear against that supplier, with severity, confidence, source and corroboration status, and why they matched.

Cyber exposure through the software you use

Major breaches and newly exploited vulnerabilities that touch the software you use, including software your suppliers provide, appear in the same picture as the physical events.

Next to your own sites

Supplier exposure sits in the same shared picture as your own sites, so the team sees how an event across your supply chain relates to your own operations.

Into your own tools

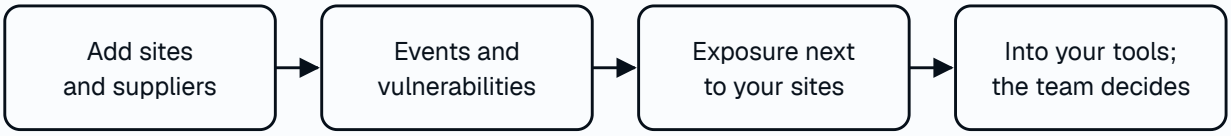
Send events into your own tools through the API and webhooks, with their evidence attached.

What you see

Item	What it shows
An exposed supplier	Which supplier, which event, the reason it matched, and the event's severity and corroboration status.
A cyber event	A major breach or newly exploited vulnerability that touches software you use, and which suppliers or sites it relates to.
Your own sites	The events that touch them, in the same picture.
An event sent through the API	The event and its evidence, in your own tools.

© Kaia Technologies, Inc.

How it works



Physical and cyber exposure across your supply chain, in one picture.

1. The resilience team adds its own sites and its key suppliers, with their facilities and the software they provide.
2. When a hazard event published by official and authoritative sources concerns a supplier's facility, the supplier appears as exposed, with the event's severity, corroboration status and the reason it matched.
3. When a newly exploited vulnerability touches software a supplier provides, it appears in the same picture, next to the sites that depend on it.
4. The event and its evidence flow into the team's own tools through the API and webhooks.
5. The team asks Hey KAIA what the exposure means for its operations. The answer cites its evidence, and the team decides its next step.

© Kaia Technologies, Inc.

Privacy and control

- Suppliers and sites sit in the organization's shared picture. Isolation between organizations is enforced at the application layer.
- The organization sees its sites and suppliers, not its people's whereabouts. Membership never grants access to another member's messages, devices, location or saved places.
- Scanning agents act only within the limits you set and with your authorization. Model output grants no authority.
- Nothing goes to cloud AI unless the person agrees first. Government organizations start with cloud AI off.

Honest boundaries

- KAIA-OR shows exposure for the suppliers, facilities and software you add.
- It does not rate suppliers or make sourcing decisions. AI informs; people decide.
- Coverage depends on what official and authoritative sources publish. Reports that cannot be corroborated are labelled as unconfirmed.
- KAIA-OR shows evidence. It does not issue an all-clear for a supplier or a site.

Editions and related use cases

Supply-chain exposure is part of the organization packages: KAIA-OR Team, Enterprise and Government. API and webhook options depend on the package. KAIA-OR runs on iOS, iPadOS, macOS, Android phones, Android TV, Windows and the web, in English, French (Canada), Turkish and Hebrew, with full right-to-left layout. One account works on every platform, with the same features and the same privacy rules.

Related use cases

- Sites and natural hazards
- Digital risk and cyber threat intelligence
- Transport and infrastructure

© Kaia Technologies, Inc.

Request early access

> Membership is by invitation. Request early access on the KAIA-OR website and choose the package that fits your organization. Enterprise and government teams can also choose Contact us on the KAIA-OR website.

© Kaia Technologies, Inc.

UCB-09-SUPPLY-CHAIN · Version 1.0 · 3 November 2026

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