ISAPHIA

PRODUCT DATASHEET

CYBER THREAT INTELLIGENCE

Threat intel that knows your attack surface.

Isaphia CTI turns generic indicators into asset-aware findings by correlating global threat feeds (CISA KEV, abuse.ch, custom sources) against the actual surface Isaphia ASM has discovered for your organization. Instead of tens of thousands of generic IOCs, your team sees the small set that maps to your real environment today.

PLATFORM CAPABILITIES

CISA KEV Correlation
Actively-exploited CVEs on YOUR surface.

IOC Relationship Graph
Pivot between indicators, assets, findings, campaigns.

TAXII 2.1 Server & Client
Push to / pull from MISP and partner collections.

EPSS Exploit Probability
FIRST.org scores on every CVE finding.

IP Reputation
GreyNoise + AbuseIPDB + VT + OTX + Shodan + Spamhaus.

MITRE ATT&CK Mapping
Per-org Navigator-compatible layer export.

Threat-Actor Landscape
Profiles + TTPs + campaigns by sector.

Hunt Page
Analyst-driven pivots + saved-search alerts.

IAB / Access-for-Sale
Forum + dark-web listings vs your assets.

Watchlists
Custom IOCs + brand / exec / project keyword watch.

Custom Feeds
RSS / JSON pull + TAXII collection ingest.

Blocklist / EDL Export
Tenant-token URL for firewall / EDR / SIEM.

Unified Risk Score
0-100 per-org score blending seven signals.

RFI Workflow
Org users raise questions; analysts answer with trail.

Allow-List / Suppression
Triaged IOCs stop re-creating findings.

Indicators Browser
Read-only global IOC store, searchable per type / source.

INTEGRATIONS & ENTERPRISE READINESS

Standards & Sharing

- STIX 2.1 + TAXII 2.1 — push & pull
- MITRE ATT&CK v14 — technique mapping + Navigator export
- CVSS v3.1 + EPSS on every CVE finding
- TLP v2.0 — RED never leaves the tenant
- JWT (RFC 7519) — short-lived API tokens with refresh
- Append-only audit log with admin-readable API

Enterprise Readiness

- Multi-tenant w/ hard per-org isolation at the query layer
- Canadian data residency (Toronto); EU / US on request
- VPC-private managed database, AES-256 at rest, TLS 1.3 in transit
- Non-root service posture, mode-600 secrets, dedicated unprivileged user
- Managed cloud database 99.95% SLA + 99.99% compute network SLA
- Scheduled intel briefs (daily / weekly / monthly per-org DOCX)

DEPLOYMENT MODELS

Standalone CTI

For SOCs already running ASM.

Plug into your existing asset graph (CMDB, Tenable, CrowdStrike) via API + watchlist seeding. Pure threat-intel-correlation use case.

ASM + CTI Bundle

One platform.

Shared asset graph, shared findings, shared alerting. The same indicators correlate against the same surface — no double-keying.

REQUEST A DEMO

isaphia.com • sales@isaphia.com •