alphaMountain

INTEGRATION BRIEF FOR MISP Threat Sharing

MISP ENRICHMENT MODULE · NOW AVAILABLE

Real-time risk ratings on every IP, domain, hostname & URL in MISP

alphaMountain now integrates directly with MISP as a native enrichment module — AI-powered risk ratings added to your network indicators without leaving the platform. No separate tool. No manual lookups. Risk context stamped on each attribute the moment you run enrichment.

01 WHY IT MATTERS

MISP doesn't tell you how dangerous an indicator is right now.

Most MISP deployments accumulate IOCs from feeds that age quickly — a blocklist entry from 72 hours ago may already be stale. alphaMountain updates **hourly**, so enriched attributes reflect the current state of that infrastructure, not a snapshot from a batch job.

The output is a **decimal risk score on the 1.00–10.00 scale** tagged directly to each attribute. Analysts set their own thresholds instead of working with binary block/allow logic.

> alphaMountain:risk-score="8.0" on a domain means what it says. It is a high-fidelity threat warning you can trust and act upon.

02 WHAT GETS ENRICHED

Any network-activity attribute, in one pass.

IPs, domains, hostnames, URLs and URIs — any attribute categorized as **Network activity**. Enrich individually, or against an entire event.

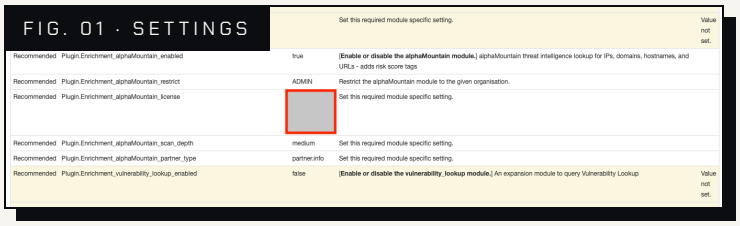
IP	DNS	URL
`ip` `ip-src` `ip-dst` `:port`	`domain` `hostname`	`url` `uri` `link`

CONFIG SETTINGS PANEL

Plugin.Enrichment_alphaMountain block.

Administration > Server Settings & Maintenance > Enrichment — set **enabled = true** and drop in your license key.

FIG. 01 · SETTINGS



			Set this required module specific setting.	Value not set.
Recommended	Plugin.Enrichment_alphaMountain_enabled	true	**[Enable or disable the alphaMountain module.]** alphaMountain threat intelligence lookup for IPs, domains, hostnames, and URLs - adds risk score tags	
Recommended	Plugin.Enrichment_alphaMountain_restrict	ADMIN	Restrict the alphaMountain module to the given organisation.	
Recommended	Plugin.Enrichment_alphaMountain_license		Set this required module specific setting.	
Recommended	Plugin.Enrichment_alphaMountain_scan_depth	medium	Set this required module specific setting.	
Recommended	Plugin.Enrichment_alphaMountain_partner_type	partner.info	Set this required module specific setting.	
Recommended	Plugin.Enrichment_vulnerability_lookup_enabled	false	**[Enable or disable the vulnerability_lookup module.]** An expansion module to query Vulnerability Lookup	Value not set.

REQUIRED — LICENSE KEY ON THE HIGHLIGHTED FIELD; EVERYTHING ELSE HAS SENSIBLE DEFAULTS.

03 HOW TO SET IT UP

Plug into MISP's native enrichment framework — four steps.

REQUIREMENT
ALPHAMOUNTAIN LICENSE ENTITLED TO THREAT ENDPOINT

01 CONFIGURE

Enable the module & add your license key.

Administration > Server Settings & Maintenance > Enrichment. Set `Plugin.Enrichment_alphaMountain_enabled` to `true` and enter your license key.

02 ADD EVENT

Create an event & add Network Activity attributes.

A new MISP event with IP, domain, hostname or URL attributes — all under category **Network activity**.

03 ENRICH

Run Enrich Event from the sidebar.

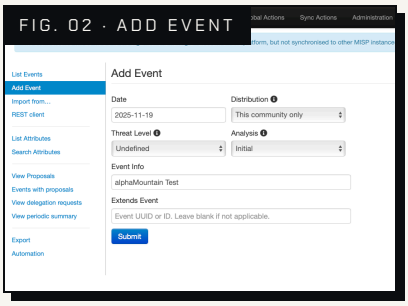
Click **Enrich Event** in the sidebar, check the alphaMountain box, hit **Enrich**.

04 READ RESULTS

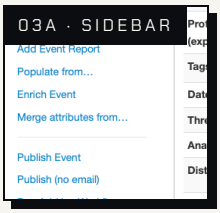
Attributes carry `alphaMountain:risk-score` tags.

Anything above your threshold is worth a closer look in **threatYeti**.

FIG. 02 · ADD EVENT



03A · SIDEBAR



03B · MODAL

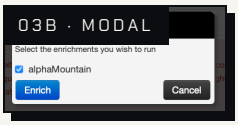
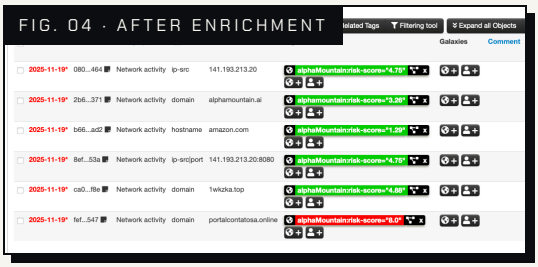


FIG. 04 · AFTER ENRICHMENT



04 · FROM SCORE TO INVESTIGATION

The score is the starting point.

When a score warrants a deeper look, the alphaMountain API and threatYeti pick up — URL classification, passive DNS, shared infrastructure, impersonation detection, and more.

CLASSIFICATION
URL category & verdict

PASSIVE DNS
Full resolution history

SHARED INFRA
IP neighborhoods

IMPERSONATION
Probability + DGA

WHOIS
Registration data

API
Automation at scale

05 GET STARTED

Three doors. Pick one.

The MISP enrichment module is available now. The fastest path is a free API trial.

01 REQUEST A FREE API TRIAL
api@alphamountain.ai →

02 INVESTIGATE ANY DOMAIN OR IP
threatYeti.com →

03 TALK TO OUR TEAM
matt.liggett@alphamountain.ai →