MODAT

CYBERSECURITY MADE IN EUROPE

INTENT LEAVES A TRACE

# Modat Magnify

Understand the intent behind internet infrastructure before it is weaponised

## The Internet Intelligence Platform

The intelligence platform that scans and catalogues the entire internet on a daily basis to identify and map every internet-connected device. By uniquely profiling each device, we turn large amounts of raw data into actionable security insights. Our AI adds context and exposes hidden relationships, evolving risks, and emerging threats.

## Get the Global Visibility You Need

Modat Magnify empowers cybersecurity analysts, researchers, product managers, and threat hunters within security teams, governments, and enterprises, as well as a growing community of thousands of security professionals. A single intelligence workspace to search, pivot and model infrastructure behaviour across IP and PassiveDNS, replacing fragmented spend across multiple tools.

## Platform Structure

| | | | | | | |
|---|---|---|---|---|---|---|
| **Teams and Agents Working With Modat Magnify** | Threat Hunting | Security Operations | Exposure Monitoring | Critical Infrastructure and OT | Digital Brand Monitoring | Fraud Investigations |
| **Built for the Agentic Era** | **M C P** Standards-Based Access for Agents | | | | | |
| **Platform Add-Ons** | PassiveDNS Intelligence | Advanced Investigation and Operations | Data and Scaling | | | |
| **Core Magnify Platform** | ■ Full IP Intelligence<br>■ Tags and Labels<br>■ Advanced Pivoting<br>■ Domain Name Search<br>■ History Comparison<br>■ Vulnerability Data | | | ■ Historical Data, One Month<br>■ Five Included Users<br>■ API Access<br>■ Customisation and Prioritisation<br>■ Custom Query and Result Volumes<br>■ Support Options | | |
| **Internet Intelligence Foundation** | Hosts | Passive DNS | Certificates | Fingerprints | Historical Records | |

MODAT

# Use Cases

One intelligence layer, every team.

## Exposure Monitoring

**THE CHALLENGE**

Teams are expected to know their full external attack surface at all times, yet most rely on periodic scans that capture a snapshot. Forgotten subdomains, exposed services and stale DNS records go unnoticed between cycles, while shadow IT and configuration drift open new entry points.

**HOW MODAT CHANGES THE WORKFLOW**

Teams work from a continuously updated map of their external footprint instead of waiting for the next scheduled scan. New assets are already discovered, exploitable misconfigurations are already flagged, and exposure is prioritised by what is attackable rather than what is merely present.

## Security Operations

**THE CHALLENGE**

SOC teams are expected to triage faster than attackers can exploit, yet analysts spend most of their time enriching alerts by hand across disconnected tools. Threat feeds produce noise as often as signal, so every investigation starts from zero and incidents are handled as one-off events.

**HOW MODAT CHANGES THE WORKFLOW**

Infrastructure context is attached the moment an alert appears, rather than assembled by jumping between the SIEM, threat feeds and ad hoc lookups. Related infrastructure is already mapped and historical behaviour is already available, so triage starts with context rather than collecting it.

## Critical Infrastructure and OT

**THE CHALLENGE**

Most OT security programmes assume the attack surface is known. It isn't. Shadow OT, devices connected without IT's knowledge, and OT systems tunnelled behind IT networks routinely stay invisible until an incident forces the discovery. IT and OT security still operate as separate disciplines, even though the networks converged years ago. What's left is a visibility gap that belongs to no single team, and by the time an attacker finds it, it isn't a surprise anymore. It's a breach.

**HOW MODAT CHANGES THE WORKFLOW**

Teams work from a continuous, internet-scale map of industrial infrastructure, including the devices nobody logged, rather than inventories that miss what was never formally provisioned. Shadow OT is already surfaced, proprietary protocols are already recognised and convergence points are already mapped.

## Threat Hunting

**THE CHALLENGE**

Hunters are expected to identify adversary infrastructure before campaigns become operational, yet investigations usually begin only after malicious activity has been observed. Manual pivoting across datasets is slow and depends on senior expertise, and by the time the infrastructure is reconstructed the attacker has moved on.

**HOW MODAT CHANGES THE WORKFLOW**

Analysts investigate from a continuously evolving model of internet infrastructure instead of pivoting across disconnected tools. Infrastructure is already clustered, historical relationships are already preserved and behavioural similarities are already identified.

## Digital Brand Monitoring

**THE CHALLENGE**

Brand teams are expected to catch impersonation, typosquatting and lookalike domains before they cause damage, yet most learn of abuse only after a customer reports it. Without continuous visibility of their own footprint, forgotten subdomains become the weak points attackers use to impersonate the brand.

**HOW MODAT CHANGES THE WORKFLOW**

Teams work from continuous visibility of both their own digital footprint and emerging impersonation infrastructure, rather than waiting for a takedown request. Lookalike domains are already flagged, related infrastructure is already connected and forgotten assets are already mapped, closing the gap attackers rely on.

## Fraud Investigations

**THE CHALLENGE**

Fraud teams are expected to stop operations before they mature, yet investigations begin case by case after fraud has occurred, because infrastructure signals (domain registrations, cloud rotation, network ties) arrive disconnected. Fraudsters rotate infrastructure quickly to exploit that fragmentation and stay out of view across incidents.

**HOW MODAT CHANGES THE WORKFLOW**

Teams work from a continuously updated, longitudinal map of infrastructure tied to known and emerging fraud actors instead of treating each case as isolated. Related domains and IPs are already connected and persistent actors are tracked across rotation. Campaign-in-formation patterns are already flagged, before the fraud reaches a customer.

MODAT

## Core Features

**Included with the core Magnify platform.**

| | |
|---|---|
| **IP and Service Details** | See all IP and service details, such as ASN, geolocation, TLS, banners, tags and fingerprints. |
| **History Search** | See a chronology of changes related to a service or host activity. |
| **Storable Custom Queries** | Store your queries and label them for future use. |
| **Tags Search** | Get access to a specific set of tags to search for. |
| **Fingerprinting Search** | Search for a specific product, technology or operating system, as well as their versions. |
| **Known Exploitable Vulnerabilities Search (KEV)** | Search for assets that are vulnerable to CVEs known to be exploited in the wild. |
| **pDNS Search** | Search for specific domain names and their IPs. |
| **CVE Search** | Search for services that are potentially vulnerable to a given CVE. |
| **File Hash Search** | Search by JS and CSS hash within web pages. |
| **OpenDir File Hash** | Search by hashes of files listed in open directories. |
| **SSO Integration** | Consolidates all application logins into a single, secure login for greater convenience and security. |

## Platform Add-Ons

**Extend the core platform as a mandate widens.**

### PassiveDNS Intelligence

**Resolution history as an investigative pillar.**

- Historical Analysis
- DNS Records Search
- WHOIS Search
- Certificate Search
- API Integration
- Advanced Pivoting
- Timeline Analysis
- Banner Analysis

### Advanced Investigation and Operations

**Each item can be added individually.**

- Threat Investigator
- TLS Fingerprint (JA3S, JA4S, JA4X, and JA4Scan-TLS)
- Regex Search
- Bulk Exports
- AI-Powered Query Assistant

### Data and Scaling

**Each item can be added individually.**

- Extended Users (Unlimited)
- Tailored Datasets (e.g. OT)
- Extra History
- Full Data Set
- On Demand Scans

## MCP

The Model Context Protocol (MCP) integration extends Modat Magnify beyond the platform by enabling connections with AI-driven workflows and external tools. This allows you to automate analysis, execute queries at scale, and accelerate investigations while continuing to use the same underlying data and query logic.

Through MCP, you can securely access Magnify data and functionality in external environments. This makes it easier to enrich investigations, automate repetitive tasks, and incorporate Magnify into broader workflows such as monitoring, enrichment, or AI-assisted analysis.

MODAT

# What We Put on the Table

## Why Security Teams Choose Modat Magnify

01

### Identity, Not Just Existence

We identify what a device is, who operates it and how it changes, backed by a database of 15K+ device profiles.

02

### From What It Is to What It Is Becoming

Continuous tracking reveals how infrastructure evolves and exposes the intent behind the changes.

03

### One Intelligence Layer, Every Team

Threat hunting, SOC, fraud, brand protection, exposure monitoring and OT security work from one shared understanding.

04

### Built for the Agentic Era

Through standards-based MCP access, agents reason over our intelligence directly, with no custom integrations.

05

### European Where It Matters Most

Fully EU-hosted and GDPR-native, providing data sovereignty by design under frameworks such as NIS2 and DORA.

06

### More Value With Every Layer

Each capability strengthens the next, so the intelligence layer grows more valuable with every investigation.

**Optimised UX and agent-ready integration.** Grouping and tagging keep search simple, so data is easy to store, pivot and reason through, and MCP integrates it with the agents already running in a customer's ecosystem.

**We build with our customers, not around them.** Every investigation and conversation shapes the platform.

# Who We Are

Modat is a European Internet Intelligence company helping organisations understand the intent behind internet infrastructure before it is weaponised. By continuously mapping, profiling and analysing internet-scale infrastructure, Modat turns fragmented data into trusted intelligence that helps security teams investigate threats faster, understand adversaries more deeply and prevent attacks before they occur. Built for both analysts and the agents they deploy, the Modat platform integrates with existing security workflows to provide the context, relationships and confidence needed to stay ahead. Governments, national CERTs, critical infrastructure operators, security companies and enterprises rely on Modat to make faster, better-informed security decisions.

INTENT LEAVES A TRACE

## What Are Attackers Already Preparing Against You?

Book a Demo

VISIT
modat.io

TRY MAGNIFY
magnify.modat.io

CONTACT
support@modat.io

CYBERSECURITY
MADE IN EUROPE

© Modat 2026 · Wilhelmina van Pruisenweg 104, 2595 AN The Hague, The Netherlands · Modat Magnify Platform Datasheet · Version 1.0, August 2026