Data Feeds & API

The signal, without the console.

FOR SECURITY ENGINEERING, DETECTION, AND THREAT INTELLIGENCE TEAMS

01 THE PROBLEM

Most domain intelligence is scraped, aggregated, and resold, which is why so many feeds agree with each other and lag the adversary together. By the time a malicious domain reaches a shared blocklist, the campaign it was built for has often already run, and the record arrives stripped of the context that would tell you what it was part of.

02 THE SOURCE

Vigilocity's feeds come from our own proprietary gathering capabilities: the same tradecraft that watches threat actors acquire and stage infrastructure for Mythic. Domains are identified as adversaries register and arm them, with the infrastructure context that separates a parked look-alike from a campaign about to launch.

03 THE API

The API is not a companion utility; it is a first-class way to consume the intelligence. Look up any domain and pivot through its registration to every domain the same registrant controls. Resolve an IP to the threats behind it. Pull DNS and data logs by date range, and stand up watchlists over the entities and network ranges you care about, with notifications when new matches appear. Everything the feeds deliver is reachable through it.

WHAT YOU GET

- Newly observed malicious domains, delivered while the campaign is still being staged
- High-confidence records with registration, infrastructure, and threat context attached
- A fully functional API for enrichment, automation, and building the signal into your own products

THE API SURFACE

01 Domain lookup and registration detail

02 Registrant pivots to related domains

03 IP lookup and associated threats

04 DNS and data logs, by date range

05 Watchlists over entities and CIDRs

06 Notifications on new matches

> An OpenAPI 3 service with key-based access, documented at docs.vigilocity.com. Nothing to deploy: the data drops into the firewalls, DNS filtering, SIEM, and TIP platforms you already run.

FRAMEWORKS ATT&CK TA0042 T1583 · TA0011 · NIST CSF 2.0 DE.CM

ABOUT VIGILOCITY

Vigilocity builds technology for identifying and eliminating threat actor infrastructure, drawing on decades of counterintelligence operations inside adversary networks.

THE METHOD

Reverse Attack Surface Analysis works from the attacker inward: tracking adversary infrastructure as it is built, then observing the victim networks that begin talking to it.

WHO RELIES ON MYTHIC

Global financial institutions, Fortune 100 brands, Big Four advisory firms, and national governments. Our clients do not appear on this page. That is part of the service.

