WHITE PAPER

Reverse Attack Surface Analysis

Watching the breach from the attacker’s side: the method behind empirical breach confirmation.

Every detection product your organization runs shares a vantage point: inside your perimeter, looking out. This paper describes the opposite arrangement. Reverse Attack Surface Analysis, RASA, is the method Vigilocity built over a decade of counterintelligence work inside adversary networks, and it watches the attack from the side of the people conducting it. The difference is not stylistic. From the attacker's side, a breach is not an anomaly to be inferred from weak signals. It is an event you can watch happen, with a timestamp.

01 The defender's blind spot

Consider what your security stack actually observes. Endpoint agents watch process behavior on machines you own. Network sensors watch traffic crossing boundaries you control. A SIEM correlates logs produced by your own systems. All of it is competent engineering, and all of it shares one structural weakness: the instruments live inside the environment they are meant to protect, which means a sufficiently capable intruder can see them, evade them, and in the worst case feed them falsehoods. The tools watching for the intruder are the first things a good intruder studies.

The result shows up in dwell time. Breaches routinely run for months before discovery, and the discovery, when it comes, often arrives from outside: a regulator, a reporter, a ransom note. Defenders are not failing for lack of effort. They are failing because inference from interior telemetry is the hardest possible way to learn a fact the adversary already knows.

There is a second, quieter consequence. Because interior tooling only covers environments where it is installed, everything outside your perimeter is dark to you. Your suppliers, your subsidiaries mid-integration, the acquisition target whose network you will own next quarter: for all of them, the traditional model offers questionnaires and outside-in scanning, which is to say, proxies.

02 Inverting the vantage point

The adversary has a perimeter too. Campaigns do not materialize; they are built, and the building materials are observable. Domains get registered. Command and control servers get stood up. Delivery infrastructure gets staged and armed. Our earlier work on the domain registration record documented what this looks like at scale: fourteen thousand domains bought by a handful of registrants over two days, reconnaissance servers assembled months before the ransomware they served, phishing fleets that follow templated naming because a human never touches them.[1]

RASA begins with that observation and follows it to its conclusion. If you index adversary infrastructure as it is acquired, continuously and at global scale, you hold a map of where attacks will come from. And once you hold that map, a breach announces itself in the simplest possible way: a victim network starts talking to infrastructure on it.

That exchange is the fact the entire method turns on. Malicious infrastructure cannot lie about who is communicating with it. The traffic either exists or it does not, and it is observed from the adversary's side of the

conversation, beyond the reach of whatever the intruder has done to the victim's own instruments. No anomaly score, no correlation across log sources, no probability. An observed, timestamped event.

03 The method

RASA rests on six pillars, unchanged since we first published them:

01	Critical time-series analysis
02	Geopolitical tension and event analysis
03	Attack surface risk profiling and rating
04	Indexing of historical global domain registration data
05	Ingestion of real-time global domain registration data
06	Correlation with open and closed source threat indicators

The pillars matter less individually than in what they combine to produce: a longitudinal record of actor behavior. The unit of analysis is never a single domain. It is the actor, over years. An operator who registers infrastructure in one burst and goes silent reads differently from one who buys six domains a day for three years, and both read differently from a brand squatter accumulating look-alikes. Time-series depth is what turns registration noise into legible intent, and it is also where operational security failures surface: the reused email address, the moniker that recurs across "unrelated" campaigns, the habit of returning to a favorite registrar. Actors tighten their discipline as they mature. The record keeps what they did before they did.

Geopolitical context does the same work at a larger grain. Infrastructure acquisition clusters around events, sanctions, elections, legislation, military movement, and reading acquisition against the calendar is often the difference between noting a spike and understanding one.

What distinguishes RASA from adversarial infrastructure analysis, its nearest relative, is the evidence it admits. Infrastructure analysis catalogs what exists. RASA also weighs indications of intent and targeting: whom the look-alike domains imitate, which sectors the staging pattern fits, where the actor's past campaigns landed. The question RASA asks is the defender's question run backward: if this adversary were coming for us, what would they need, when would they acquire it, and from where would it originate?

04 From signal to evidence

Prediction has a ceiling. Knowing a campaign is assembling tells you to raise your guard; it does not tell you whether the campaign reached anyone. So the second half of the method watches the infrastructure in operation, and this is where Mythic, the platform built on RASA, does its work.

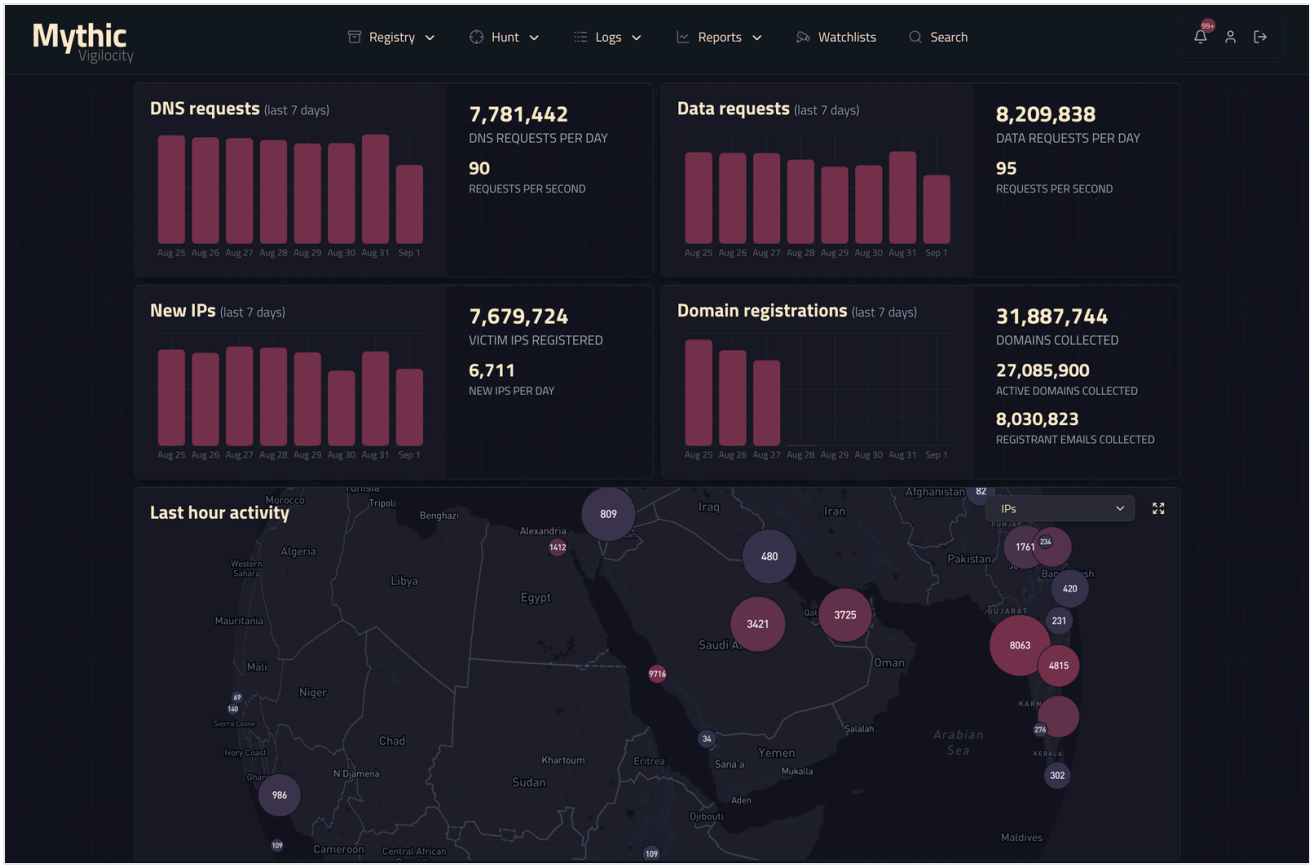

FIG. 1 The Mythic console: confirmed breach activity, ranked by material impact.

When a victim network begins communicating with tracked infrastructure, Mythic records the exchange itself. Each confirmed breach carries the date and time of the observed communication, the victim and destination IP addresses, the port and protocol in use, the data exfiltrated by the implant, the machine, user, operating system, and file paths involved, and the implant responsible. That bundle is the difference between an alert and evidence. An alert asks a security team to go find out whether something happened. Evidence tells a general counsel what happened, when, and to which systems, in a form that survives scrutiny.

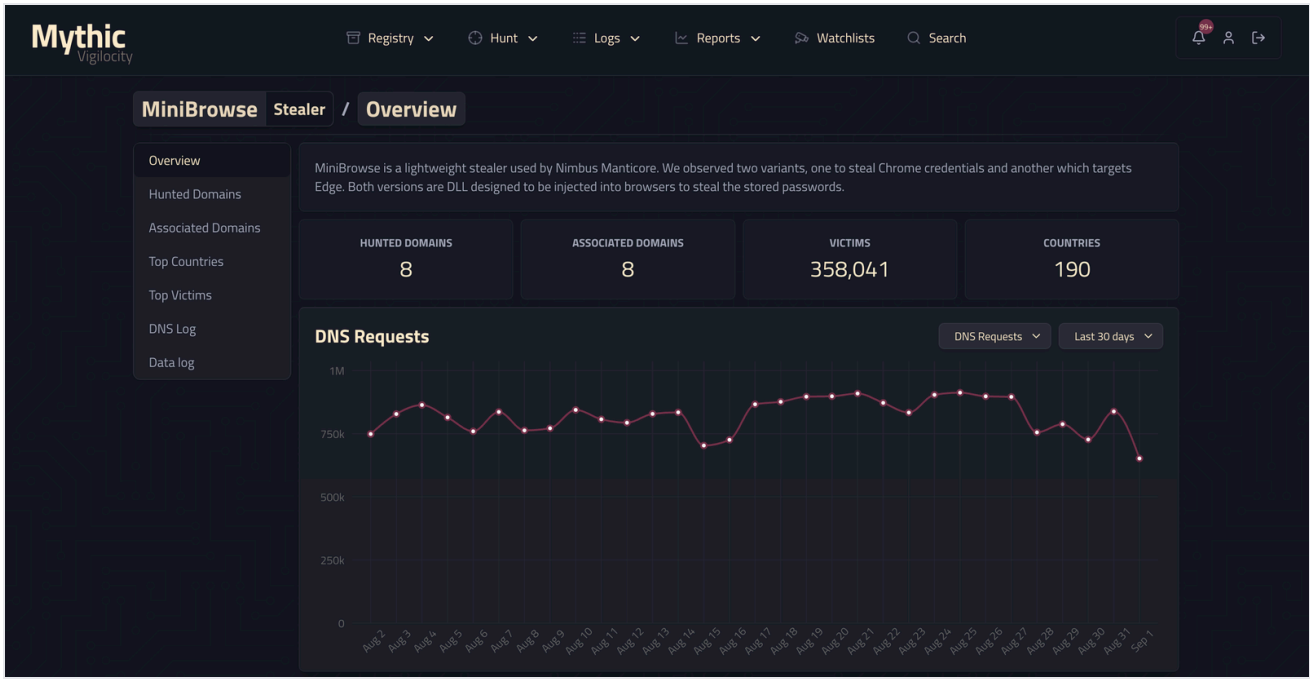

FIG. 2 A confirmed breach record: the observed exchange, the implant, and the exposure, with evidence attached.

Volume is the enemy of judgment, so Mythic ranks what it confirms. Materiality models weigh what is actually being taken, from whom, and at what apparent rate, so that a security team, a disclosure committee, or an underwriter starts each morning with the incidents that matter rather than a queue sorted by recency. The ranking is a lens over the evidence, never a substitute for it; the underlying observation rides with every record.

05 What agentless actually buys you

Nothing in the preceding two sections touches the subject organization. No agent, no appliance, no API credential, no questionnaire. The observation happens on the adversary's side of the exchange, which has a consequence that is easy to state and slow to sink in: the subject of an assessment does not need to participate in it, or even know it is occurring.

For your own organization this means coverage that an intruder cannot blind by compromising your tooling, because the collection does not run on anything you own. For everyone else it means the assessment boundary disappears. A vendor can be evaluated with the same rigor as your own network. So can an acquisition target during diligence, quietly, without tipping the target's staff. So can an insurance applicant at underwriting, or an entire book of insureds, continuously, between renewals. The traditional distinction between organizations you can assess and organizations you must trust reduces to a single question: are their networks in contact with adversary infrastructure, or not.

Honesty requires the converse statement too. RASA is not an endpoint product and does not pretend to be one. It does not patch systems, quarantine machines, or replace the interior stack; remediation still happens inside the perimeter, by the people who own it. Its coverage is of the infrastructure Vigilocity tracks, which is vast and continuously refreshed but is not a census of everything hostile on the internet. What the method claims, and

what a decade of operating it supports, is narrower and more useful: when a network under observation talks to tracked adversary infrastructure, that fact is known, with evidence, at the time it is true.

06 Where the method lands

The applications follow directly from the two properties, observation and non-participation. Public companies use the evidence to run materiality determinations on the SEC's four-business-day clock, on facts rather than forensic estimates. Third-party risk programs monitor entire vendor populations continuously, the long tail included, instead of interviewing the top twenty annually. Carriers price cyber risk against observed compromise rather than self-attestation, and watch portfolios for accumulation between renewals. Deal teams answer the one diligence question that questionnaires structurally cannot: is this target compromised right now?[2]

Different desks, same underlying fact pattern. In each case a decision that used to rest on proxies, scores, attestations, scans, assurances, now rests on whether an exchange was observed. That substitution, proxies out, observation in, is the whole of the method's ambition.

07 Conclusion

Security tooling has spent thirty years refining the same vantage point. The returns on that refinement are real, and diminishing. RASA's wager is that the next meaningful gain comes from standing somewhere else: on the infrastructure the adversary believes is invisible, watching it get built, and watching who talks to it. From that position, prediction and confirmation stop being separate disciplines. They are the same record, read at two moments in time.

08 Sources

1. Vigilocity, "Geopolitical Cyber Event Prediction: Using Reverse Attack Surface Analysis," second edition, 2026. vigilocity.com/resources
2. U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," 17 CFR Parts 229, 232, 239, 240, 249. Item 1.05 of Form 8-K requires disclosure of material cybersecurity incidents within four business days of a materiality determination.

ABOUT VIGILOCITY

Vigilocity builds technology for identifying and eliminating threat actor infrastructure, drawing on decades of counterintelligence operations inside adversary networks. Its platform, Mythic, confirms material breaches by observing them from the adversary's side.

BRIEFINGS

Request a briefing

vigilocity.com/contact