Third-Party Risk

Assess any partner from a distance. No questionnaire, nothing deployed.

FOR TPRM, VENDOR RISK, AND SUPPLY CHAIN SECURITY TEAMS

01 THE PROBLEM

Third-party risk programs run on borrowed evidence. Questionnaires measure a vendor's ability to answer questionnaires. Security ratings score the hygiene visible from outside: open ports, patch cadence, certificate discipline. Both are proxies, and neither observes the one event the program exists to catch: a partner whose network is in live contact with an adversary.

02 THE APPROACH

Mythic observes it directly. Because collection happens on the adversary's side of the exchange, assessing a third party requires nothing from the third party. No agent on their endpoints, no access to their environment, no questionnaire in their inbox. If their networks are talking to infrastructure Mythic tracks, that fact is visible from a distance, the day it becomes true.

03 IN PRACTICE

Traditional diligence is expensive enough that most organizations assess a handful of critical vendors annually and accept blindness on the rest. Mythic watches the entire population continuously, the long tail included, and surfaces the supplier that matters this week, ranked by what is actually being taken. When the signal fires, the vendor conversation starts from timestamped evidence rather than suspicion.

FRAMEWORKS NIST CSF 2.0 GV.SC · ISO 27001 A.5.7 · ATT&CK TA0042

WHAT YOU GET

- Assessment of any third party without their participation
- Continuous monitoring of the entire vendor population, not an annual review of the top twenty
- Early warning when a critical supplier is in live contact with adversary infrastructure

EVERY CONFIRMED BREACH CARRIES

01 Date and time of breach
02 Victim and destination IPs
03 Port and protocol
04 Data exfiltrated by the implant
05 Machine, user, OS, file paths
06 The implant responsible

> Nothing to install, no hardware, no access to any environment required. Mythic observes from the adversary's side of the exchange.

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.

