# Breach Disclosure & Materiality

The four-day clock starts when you know. Know first.

FOR CISOS, GENERAL COUNSEL, AND AUDIT COMMITTEES AT PUBLIC COMPANIES

## 01 THE PROBLEM

Public companies are obligated to disclose material cybersecurity incidents on a short, unforgiving clock, and the hardest part of that obligation is not the filing. It is knowing, with evidence, that a material breach has actually occurred.

## 02 THE APPROACH

Mythic observes breaches from the attacker's side. Because it watches adversary infrastructure rather than your endpoints, it produces empirical evidence of compromise: which of your networks are communicating with malicious command-and-control infrastructure, when the contact began, and how severe the exposure is. None of it depends on the very systems an attacker may already control.

## 03 IN PRACTICE

That evidence gives disclosure teams a defensible, documented basis for materiality decisions: to disclose promptly when the facts warrant it, and to avoid over-disclosing when they don't. Each confirmed breach carries the observed exchange itself, timestamped, with the data taken and the infrastructure responsible.

FRAMEWORKS SEC Cyber Disclosure · NIST CSF 2.0 RS.CO · GDPR Art. 33

## WHAT YOU GET

- Independent confirmation of material breach, backed by observed communication
- Evidence packages that support materiality determinations under SEC disclosure rules
- Continuous monitoring, so the first word of a breach never comes from a regulator or reporter

## 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.

 