If an attack is prevented, do we still have to report a breach?

Short answer: Generally no. When an attack is stopped before execution and no data is accessed, altered, or exfiltrated, there is typically no breach to disclose. Disclosure obligations are usually triggered by unauthorized access to protected data — not by an attempt that failed.

A real example

In the financial services deployment where Cyber Crucible intercepted nearly 10,000 malicious processes, the outcome for the CISO included zero regulatory disclosure. Because the attacks were stopped pre-execution and no data was touched, there were no required notifications to customers, vendors, or government regulators — and no headlines, which preserved customer trust.

An important caveat

Disclosure requirements vary by jurisdiction, industry, and contract, and the specific facts of an incident matter. Cyber Crucible is not a law firm and this is not legal advice. The reliable principle is that prevention narrows your disclosure exposure dramatically compared with detection-after-the-fact — but your counsel and compliance team should make the determination for any given event.

Revision #3
Created 2026-07-20 19:24:04 UTC by Dennis Underwood
Updated 2026-07-21 19:32:19 UTC by Dennis Underwood