ANATOMY OF A BAD DAY · 1 OF 6

The worst day of a CISO's career starts at 3:07 AM.

But it didn't begin there.

THE CALL

The call comes in: *anomalous outbound transfers,* and they've been running for weeks.

Here's the part nobody tells you — by the time the phone rings, the breach is already **14 months old.**

RUN THE TIMELINE BACKWARD

3:07 AM, today
Detection finally fires.

6 weeks ago
A buyer acts on the access. Bulk exfiltration begins.

11 months ago
The attacker logs in with a valid credential. No alarm — the login was *legitimate*. The access is parked, then sold on.

14 months ago
That credential is phished, scraped, or simply found.

3 years ago
Someone decided a permanent credential was an acceptable way to reach sensitive data.

THE ACTUAL BAD DAY

> Credential-based breaches average **~292 days** to identify & contain — the longest of any vector.
> IBM, Cost of a Data Breach 2024

THE REFRAME

We treat the 3 AM call as the bad day, and the architecture decision as background noise.

It's the opposite. **The bad day was the decision.** Everything after was just the invoice arriving.

OVER THE NEXT TWO WEEKS

The bad days that show up in real post-mortems —

> *the bypassed MFA*
>
> *the mis-sent file*
>
> *the vendor's “we regret to inform you” email*

— and the **architecture choice, years earlier,** that each one traces back to.

THE PATTERN

Nobody has a bad day the moment they make a bad architecture decision. They have it later — at 3 AM, when the decision finally collects.

Preventing bad days is the whole job.