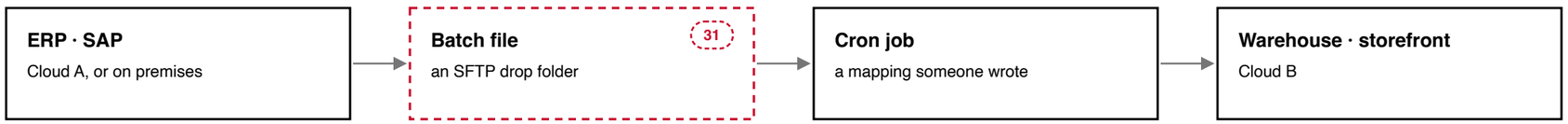
FROM CRON TO AGENTS — WHO BINDS THE SYSTEMS, AND WHERE SECURITY HAS TO LIVE

binding moved from build time, to event time, to runtime; security has to stay where the model can't reach it

Red dashed = a gap. Numbers and letters match the security gaps article.

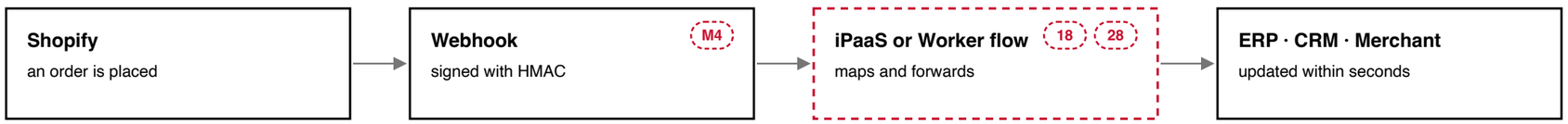
THREE ERAS OF MOVING DATA BETWEEN SYSTEMS

1 · Cron EDI and ETL — binding at build time, data moves on a schedule



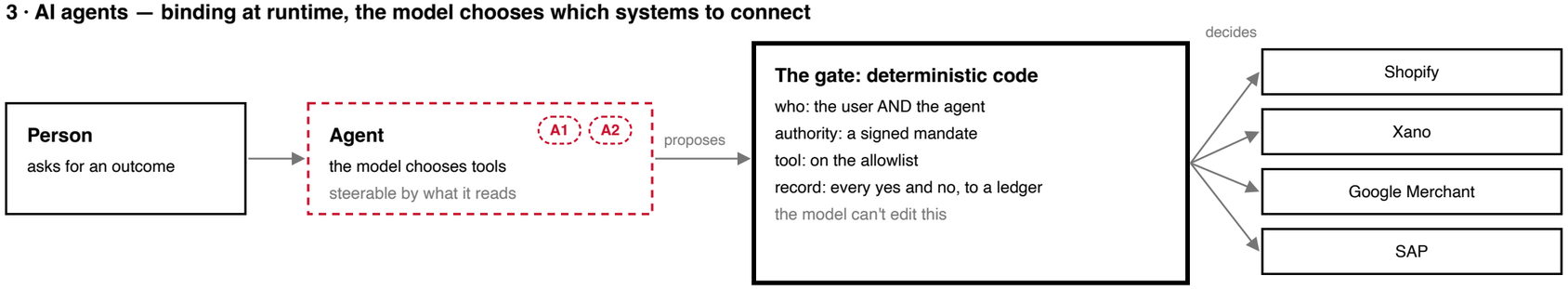
WHO BINDS	a developer, and a reviewer
WHEN	on a schedule: nightly, or every 15 minutes
SECURITY	the perimeter, SFTP, the reviewed mapping
FAILS	files at rest in plaintext; stale data

2 · APIs and iPaaS (integration platform as a service) — binding at integration time, data moves per event



WHO BINDS	integration code, or an iPaaS flow
WHEN	per event, in real time
SECURITY	API keys, scopes, signed webhooks
FAILS	broad keys; middleware keeps copies

3 · AI agents — binding at runtime, the model chooses which systems to connect



WHO BINDS	a model, choosing tools at runtime
WHEN	per request, decided on the fly
SECURITY	the gate, outside the model
FAILS	without it: injection, excessive agency, token passthrough (A1, A2, A3)

WHERE SECURITY HAS TO LIVE — FOUR THINGS THE MODEL CAN'T REWRITE

1 · The data — M3, 20

Consent state is a field on every record. A record without it is refused, whoever asks.

2 · The identity — A3

The user and the agent are each identified. Every token is scoped to one tool's audience.

3 · The authority — A4

A signed mandate: amount, merchant, expiry and a one-time nonce, checked per call.

4 · The gate — A7

Code at the endpoint says yes or no, and writes every grant and denial to an append-only ledger.

THE THREE ERAS SIDE BY SIDE

ERA	WHO BINDS THE SYSTEMS	WHEN	WHERE SECURITY LIVED	WHAT FAILS
Cron EDI / ETL	A developer's mapping, reviewed	On a schedule	The perimeter, SFTP, the mapping	Plaintext batch files (31), stale data
APIs and iPaaS	Integration code or iPaaS flows	Per event, in real time	API keys, scopes, signed webhooks	Broad keys (M1), middleware copies (18, 28)
AI agents	A model, choosing at runtime	Per request, on the fly	Outside the model: a deterministic gate	Injection (A1), agency (A2), passthrough (A3)

The model proposes. Deterministic systems decide. Every grant and denial is recorded.