THREATIQ | LABS

THREATIQ LABS FIELD NOTES

Detection Engineering for Security Leaders

Why reliable detection is a program you run, not a product you buy.

FIELD NOTE #003

THE PROBLEM

You can’t buy your way to good detection.

Most organizations assume that deploying a SIEM or EDR — with its library of built-in rules — means detection is handled. It isn’t.

Detection is not a feature you enable. It’s a capability you build.

Vendor rules are built for broad applicability, not your reality. The result is predictable: too much noise and too little signal.

Environments evolve constantly. New systems appear, log formats change, business processes shift. A rule that worked last quarter can quietly stop firing — and you may not discover it until after an incident.

Every detection has an expiration date.

The question is whether you’ll notice before an attacker does.

WHY AD-HOC DETECTION FAILS

Why most detection quietly breaks.

01

No ownership

Rules get written reactively after an incident, by whoever’s available, then forgotten. No one is accountable for whether they still work.

02

No lifecycle

Detections aren’t versioned, tested, or tuned. They rot as data sources and attacker behavior change over time.

03

No measurement

Teams can’t say what their coverage is, which rules are noisy, or what’s actually firing. You can’t improve what you don’t measure.

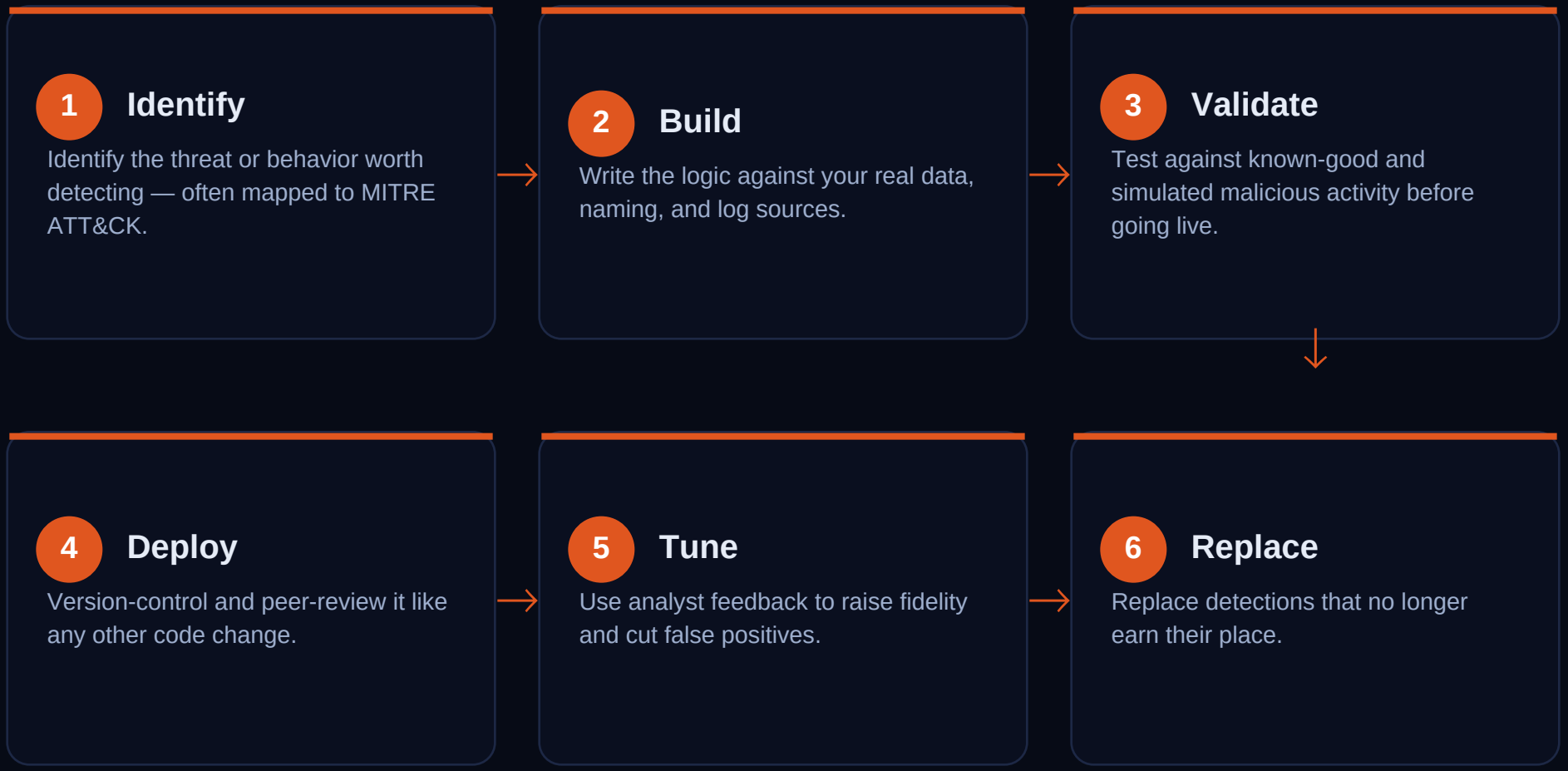
Detection isn’t a configuration task.

It’s an operational discipline that requires ownership.

RUN DETECTION LIKE SOFTWARE

The detection lifecycle.

Mature programs treat every detection as code — built, tested, and maintained through a repeatable lifecycle.



Reliable detection isn’t built through heroic effort. It’s built through repeatable process.

WHAT DETECTION-MATURE LEADERS INSIST ON

Five things to insist on.

Ownership

Every detection has a named owner accountable for its health.

Engineering discipline

Detections are version-controlled, peer-reviewed, and tested like code.

Coverage mapping

Detections map to a framework so gaps are visible.

A tuning loop

Analyst feedback keeps improving fidelity — tuning is never done.

Measurement

Coverage, false-positive rate, and time-to-detect are tracked over time.

Detection engineering turns scattered alerts into a measurable capability — one you can trust, improve, and defend to the board.

Anyone can buy alerts.
Confidence has to be engineered.

ThreatIQ Labs Field Notes — helping organizations turn telemetry into trusted intelligence.

info@threatiqlabs.com · **threatiqlabs.com**