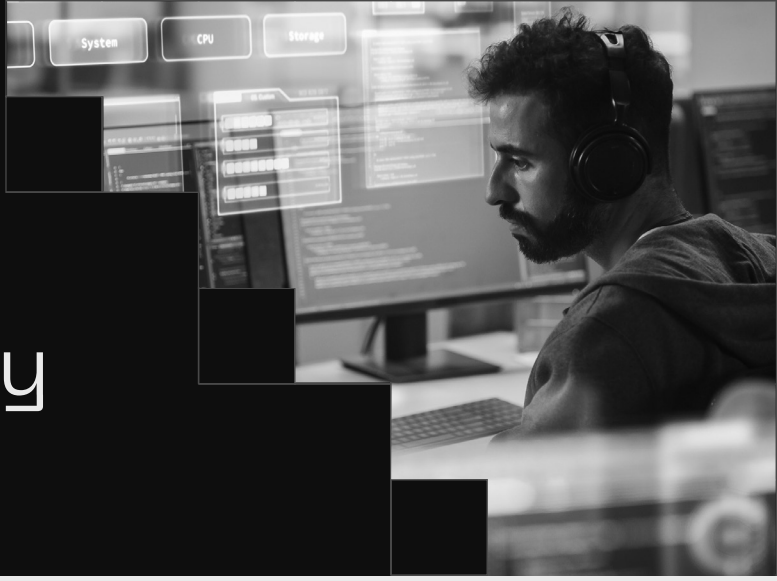
DATASHEET

Threat-Informed Detection Strategy Overview

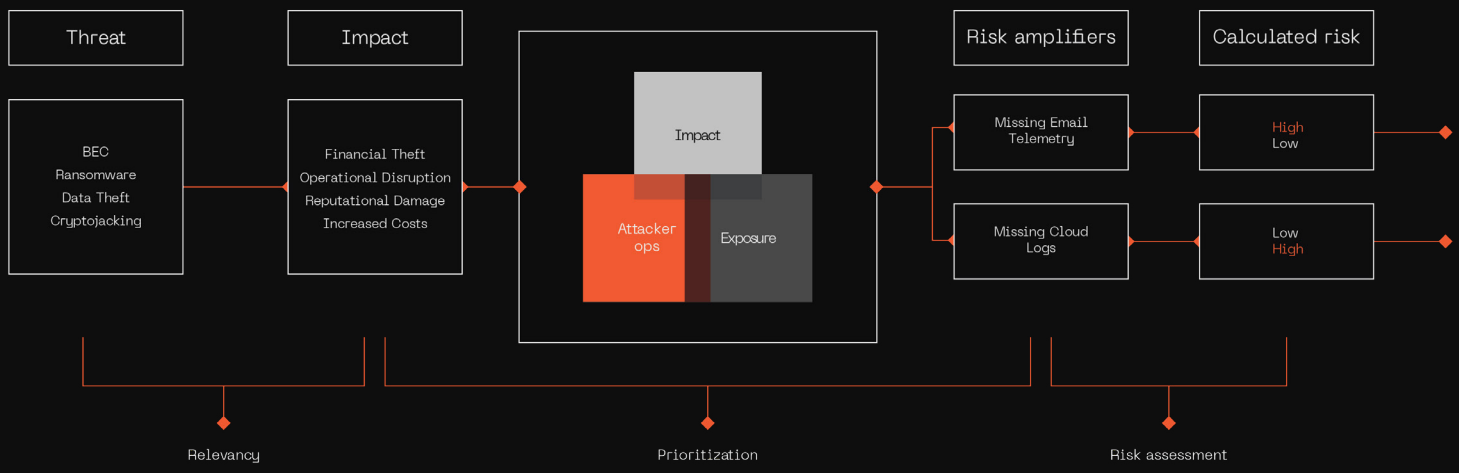


Flipping the playbook to think like attackers, defend like experts.

Why Threat-Informed Defense Works

Traditional detections are often generic, reactive, and noisy. At Binary Defense, we don't build detections in a vacuum; we build them like attackers would. Our Threat-Informed Detection Engineering (TIDE) strategy flips the playbook, applying the Attackers' mindset to engineer defenses that stop real threats, not just surface-level activity. We model and replay attacks to target the right data and the most impactful attack stages.

From low-risk automations to full-force analysis, our approach scales with impact and delivers clarity over noise.



The TIDE Approach

TIDE reframes detection engineering through an evidence-based lens. It asks engineers to think like researchers: to begin each detection with a threat models, gather supporting evidence from available telemetry, design an experiment to validate it, and only then deploy the logic into production.

In this model, detections become scientific artifacts, each one traceable to a threat model, test results, and validation evidence.

Core Principles

Our detection engineers are analysts who have sat in the hot seat and use that perspective to build meaningful, high-fidelity detections. Every environment is mapped against adversary tactics, techniques, and procedures (TTPs) to create tailored detections for your business and sector.

- Threat-Informed Defense: Built from real adversary behaviors, not guesswork.
- Intelligence-Driven: Powered by threat intelligence, MITRE ATT&CK mappings, and insights from live hunts.
- Context Over Volume: Every alert has purpose and relevance, reducing noise and elevating what matters most.
- Practical Engineering: Works with your existing tools and maturity—no rip-and-replace required.

What Sets Us Apart

Industry-Specific Profiles
We align detections with attacker behaviors targeting your vertical—finance, healthcare, manufacturing, or tech. You get protection built around your threat exposure.

Maximize Existing Investments
We design logic that fits your visibility and environment, helping you get more out of your current security stack.

Grounded in Experience
Our engineers and analysts know the flood of meaningless alerts. That's why we focus on clarity, context, and stopping high-impact events before they happen.

Partnership Over Handoff
We're not just here to send alerts. We're here to collaborate, strengthen defenses, and put you back in control.

The Outcome
With TIDE, you don't just detect threats—you detect the right threats.

You gain:

- Higher fidelity detections tailored to your environment.
- Clear visibility into where your defenses are strong and where gaps exist.
- Alerts that cut through the noise, backed by intelligence and real-world hunting.
- A partner committed to helping you out-maneuver adversaries, not just chase them.

Threat-Informed Detection Engineering represents a paradigm shift in how defenders conceptualize and construct their detection capabilities.

By aligning intelligence with engineering discipline, it moves the practice of detection from an art form to an empirical science that is governed by data, process, and continuous validation.

600 Alpha Parkway, Stow OH 44224
sales@binarydefense.com

BINARY DEFENSE