DATASHEETv

Threat-Informed Detection Strategy (TIDE): Technical Datasheet

Precision-Built Detections for a Noisy World.

Why TIDE

Traditional detection programs emphasize rule quantity over quality, leading to alert fatigue, false positives, and missed attacks. TIDE reverses that equation by treating detection creation as a true engineering discipline. Every detection is threat-modeled, evidence-based, and validated through automation before deployment.

The result is a precision-built detection ecosystem that evolves with the threat landscape and delivers high-fidelity signals aligned to real attacker behavior.

Traditional Detection Engineering	Threat-Informed Detection Engineering
Static rules built from intuition	Threat-modeled hypotheses derived from real attacker behavior
Manual rule updates and drift	Detection-as-Code (DaC) with peer review and CI/CD automation
Alert fatigue and false positives	Empirical validation and fidelity scoring
Stagnant visibility	Continuous improvement loop guided by telemetry feedback

Key Benefits:

- Precision detections aligned to real attacker behaviors
- Ongoing refinement as the threat landscape evolves
- High signal-to-noise ratio to reduce analyst fatigue
- Continuous validation and automation pipelines

TIDE Core Principles

Intelligence as Design Input:

Every detection starts with actionable threat intelligence. Engineers translate adversary TTPs into detection requirements that prioritize real, high-impact behaviors.

Threat Modeling & Hypothesis Testing:

Detections begin with the development of threat models that are emulated in a controlled environment. Observations are taken to craft a formal detection hypothesis, which is then validated and ultimately refined until the detection produces consistent, explainable results.

Detection-as-Code (DaC):

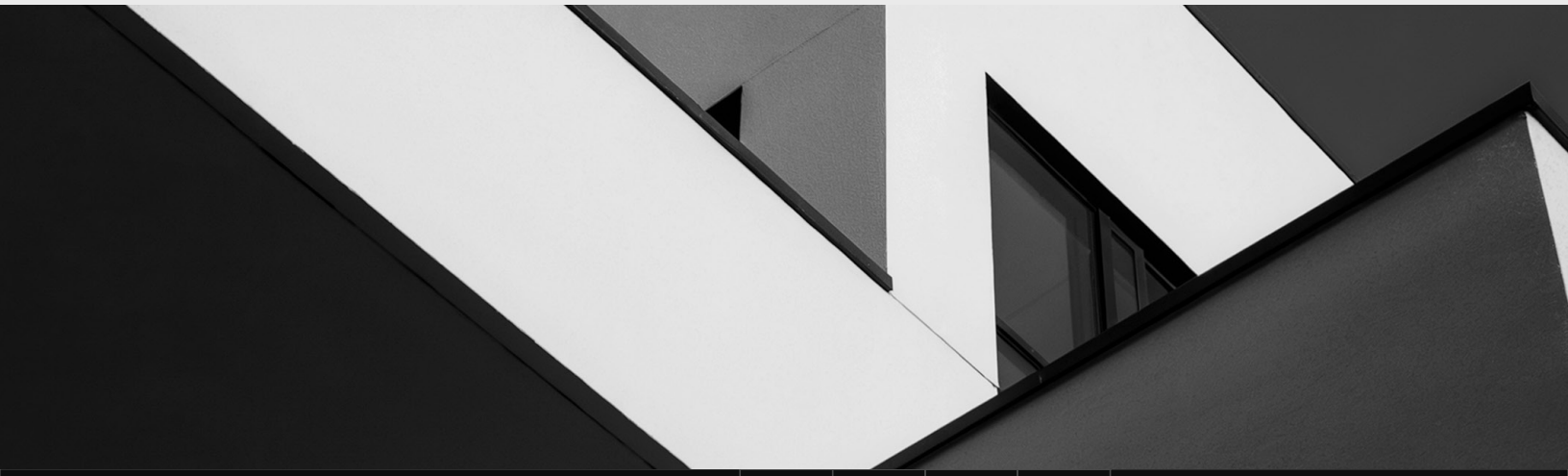
Detections are built, versioned, and deployed like software—enabling collaboration, traceability, and rapid automation.

Continuous Validation & Metrics:

Each detection is tracked against key performance metrics to ensure continued reliability, even as environments and attacker tactics evolve.

TIDE Powers Binary Defense's MDR Solution

Every detection starts with actionable threat intelligence. Engineers translate adversary TTPs into detection requirements that prioritize real, high-impact behaviors.



The TIDE Workflow

Define Threat Priorities

Identify adversaries and high-impact TTPs based on threat intel and internal telemetry.

Formulate Threat Model

Apply GOST (Goal, Objective, Strategy, and Tactics) to map attacker goals to observable behaviors and telemetry.

Build Detection Logic

Develop detection YAMLs using standardized schemas and peer review to maintain consistency.

Validate Through Testing

Simulate attacker techniques using Atomic Red Team and Caldera. Measure fidelity, tune false positives, and record validation data.

Deploy via CI/CD

Automate deployment to SIEM, EDR, or XDR systems with version control and rollback assurance.

Measure & Refine

Track fidelity, coverage, and drift metrics to guide ongoing improvement and tuning.

TIDE Empowers Your Team

Your Goal	How TIDE Helps You Achieve It
Reduce noise and alert fatigue	Empirical validation and fidelity scoring remove excess alerts
Strengthen visibility	Threat-modeled detections mapped to MITRE ATT&CK
Improve SOC performance	Analysts receive fewer, richer, context-ready alerts
Future-proof detection coverage	CI/CD pipelines ensure detection logic evolves automatically

The result of TIDE is a living system that learns, adapts, and strengthens with each iteration. Detection becomes not a static rulebook, but a dynamic reflection of the threat landscape itself.

TIDE transforms threat intelligence into engineered resilience.

Binary Defense is a trusted leader in Managed Detection and Response (MDR), helping organizations across industries stay ahead of modern cyber threats. Our team of SOC analysts, threat hunters, detection engineers, and researchers works around the clock to deliver outcomes that matter: earlier threat detection, faster response, and stronger long-term security.

We take an attacker's mindset to defense, combining deep expertise with proactive tradecraft to protect what matters most.

Learn more at binarydefense.com, explore our blog for the latest insights, or follow us on LinkedIn.

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

BINARY DEFENSE