DORAHACKS REACTIVE OMNI BUILDATHON · TRACK: EVERY SECOND COUNTS

OmniGuard AI V2

Autonomous Cross-Chain DeFi Risk Sentinel & Hardened Reactive Omni Guardrail Engine

VERIFIED LIVE EXECUTION + V2 SECURITY HARDENING + ZERO-SETUP JUDGE WORKBENCH

OmniGuard AI listens to Base Sepolia (200ms Denim blocks) and Unichain Sepolia (1s blocks) via Reactive Lasna (~1s CometBFT finality), evaluates rules and EIP-712 neural advisements in Solidity, and dispatches authenticated cross-chain callbacks without centralized keeper bots.

2s / 3s	7,155 ms	29 / 29 PASS	0 High / 0 Med
Confirmed On-Chain Block Deltas	Measured End-to-End Wall Clock	Foundry + 128k Invariant Calls	Aderyn + Slither + Gitleaks

PUBLIC JUDGE LINKS (1-CLICK VERIFICATION, ZERO CLONE REQUIRED)

Live RPC Workbench & Breaker Lab:	https://alphonshhhomenicmtu.github.io/omniguard-ai/
1080p Demo Video (2m30s):	https://youtu.be/pggBrUXMLTo
Source Repo & Contracts:	https://github.com/alphonshhhomenicmtu/omniguard-ai
DoraHacks BUIDL:	https://dorahacks.io/build/51789

02 · PROBLEM STATEMENT

Why 200ms Rollups Break Legacy Keepers and 7s Relayers

Base Sepolia Denim (200ms blocks) and Unichain (1s Flashblocks) compress liquidation windows into seconds

1. Sub-Second Cascades

A 6% WETH drawdown on a 200ms L2 triggers liquidations across dozens of blocks before legacy ~7s reactive networks even finalize the origin log.

2. Block-Number Timer Drift

Contracts using block.number for cooldowns assume 2s L2 blocks. On Base Sepolia's 200ms cadence, a 15-block cooldown expires in 3 seconds instead of 30s, causing double-hedging.

3. Polling Bots Are Not Agents

Off-chain cron scripts polling RPCs and signing vault txs introduce single points of failure, opaque keys, and gas failures during volatility spikes.

OMNIGUARD PRINCIPLE: THE AGENT PROPOSES, THE REACTIVE CONTRACT COMMITS

Our neural risk model only emits EIP-712 signed advisements. All subscription matching, cooldown checks (strictly uint64 Unix timestamps), adaptive threshold tightening, and authenticated destination callbacks execute deterministically inside OmniGuardReactive on Reactive Lasna and OmniGuardVault on Unichain/Base.

End-to-End Architecture Across 3 Live Testnets

Built natively on Reactive-Network/reactive-lib-omni (SYSTEM 0x8888...8888 + ERC-1967 CallbackProxies)

1. ORIGIN FEEDS

Base 84532 & Unichain 1301

OmniMarketFeed.sol

`0xd30a...0f80 (live)`

- PriceUpdated (opCode=2)
- HealthFactorAlert (opCode=3)
- NeuralRegimeCommitted

`EIP-712 ecrecover + <=180s TTL`

->

2. REACTIVE LASNA

Chain 5318007 (~1s CometBFT)

OmniGuardReactive.sol

`0xb04f...5ef6 (live)`

- AbstractReactive (onlySystem)
- Multi-topic subscribe()
- Adaptive AI drawdown tightening
- requestCallbackV_1_0(address(0))

->

3. DESTINATION VAULTS

Unichain 1301 & Base 84532

OmniGuardVault.sol

`0x5b10...380c (live)`

- AbstractCallback dual auth:

`onlyServiceProvider +`

`onlyCallbackSender`

- On-chain ExecutionReceipt log

VERIFIED OMNI SYSTEM & PROXY PARAMETERS (NO LEGACY PRE-OMNI ADDRESSES)

Lasna SYSTEM:	0x8888888888888888888888888888888888888888	(extraGas 100k, maxCharge 50k)
Base Proxy:	0x476F44b11F5C942c58f4c8E3d0300E5710743585	(extraGas 80k + 50k -> V2 floor 450k)
Unichain Proxy:	0x775c9B990ADe401060B78D0e98684eEf8d2466C1	(160-bit first-arg sender injection)

04 · LIVE ON-CHAIN EXECUTION PROOFS

Two Confirmed Full-Loop Executions on Testnet

Verified directly on Base Sepolia (84532) -> Reactive Lasna (5318007) -> Unichain Sepolia (1301)

LOOP #1 — RULE #1 STOP-LOSS HEDGE (-6.00% WETH CRASH -> 50% HEDGE) · 2s ON-CHAIN DELTA

Origin Tx (Base 84532, blk 62980986, ts 1795518066): 0x1155b750cbe38ef1ede5727ef1819f7b8fd50625366c836a887e555a83243dd2

Reactive Tx (Lasna 5318007, blk 9131928): 0x34598c2fb358b08bfb9ea5e6213f9377c33226db193fd29f4f0a0559355d2e9f

Callback Tx (Unichain 1301, blk 68665640, ts 1795518068):0xcb2cb194a1c4a561e911e253832021d8a9c3e8b6be3de9a87090f7e7fb8b1f4c

Decoded Unichain getReceipt(0): $100,000 WETH -> $50,000 WETH | $25,000 USDC -> $75,000 USDC | Debt $60,000 | Latency = 2s

Measured end-to-end script wall clock (broadcast + RPC confirmation + 1s log polling): 7,155 ms.

LOOP #2 — RULE #3 EIP-712 NEURAL CIRCUIT BREAKER (91.2% RISK -> 65% SHIFT) · 3s ON-CHAIN DELTA

Origin Tx (Base 84532 EIP-712 ecrecover, ts 1795518068):0xb11c83b3b5893ab11209c8f2fb0efd62c3f25bc3d7e2585737cd360e288b7f37

Reactive Tx (Lasna 5318007, blk 9131931): 0xdb6d3164304d8e7c24e92803bd36e0e0c3b70e3e0b443c1e4113adc97f21c428

Callback Tx (Unichain 1301, blk 68665643, ts 1795518071): 0x60a450775431b9f27b2065b138cc6cfd737642ad31b16b3f92efd1e9ba7783c2

Decoded Unichain getReceipt(1): $50,000 WETH -> $17,500 WETH | $75,000 USDC -> $107,500 USDC | Debt $60,000 | HF ~1.94x

Re-read live anytime in Tab 1 of https://alphonshhhomenicmtu.github.io/omniguard-ai/ directly via Unichain public RPC.

05 · HONEST LATENCY TELEMETRY

Separating Block-Timestamp Deltas From Wall-Clock Polling

Clear engineering reporting: measured chain timestamps, measured RPC wall-clock, and modeled legacy baseline

Loop #1 (Base -> Lasna -> Unichain) — 2 seconds [MEASURED ON-CHAIN]

Exact callbackTimestamp (1795518068) minus originTimestamp (1795518066) stored in Receipt #0.

Loop #2 (EIP-712 Neural -> Unichain) — 3 seconds [MEASURED ON-CHAIN]

Exact callbackTimestamp (1795518071) minus originTimestamp (1795518068) stored in Receipt #1.

Full Script Wall-Clock (last-proof.json) — 7.16 seconds [MEASURED WALL-CLOCK]

Includes Base Sepolia RPC broadcast confirmation, Reactive Lasna relay, and 1,000ms destination log polling.

Legacy Pre-Omni Reactive (~7s blocks) — ~8.6s - 9.5s [MODELED BASELINE]

Pre-Omni 7s finality adds ~6s of reactive confirmation delay before a callback can even be queued.

Candid V1 Audit Findings and Exact V2 Remediation

We ran an adversarial red-team review plus Aderyn, Slither, and Foundry stateful fuzzing on our own V1 contracts

C1 (Critical): Permissionless createRule()

V1 Gap: V1 let any wallet register rules against the shared Unichain vault and burn lREACT into InDebt.

V2 Fix: V2 adds onlyRuleCreator allowlist, allowedDestinationVaults[chainId][vault], 8/market (32 total) cap, swap-and-pop pruning, and owner pause().

C2 (High): Inert Circuit Breaker & No-Op Action

V1 Gap: V1 set circuitBreakerActive=true but never checked it; executeProtection accepted action 3 as a no-op.

V2 Fix: V2 hard-reverts executeProtection & executeCrossChainRebalance when circuitBreakerActive, adds 4-action/hr cap, and binds RuleKind <-> ActionType.

H1 (High): Unbounded EIP-712 TTL & Fallback Key

V1 Gap: V1 allowed unbounded validUntil and agent/eip712Signer.ts fell back to a public Anvil key.

V2 Fix: V2 caps validUntil <= now+180s, issuedAt skew +/-120s, clears snapshots on signer rotation, and fails closed when signer key is missing.

M1 + Static Analysis (Aderyn / Slither)

V1 Gap: V1 had 250k gas floor, replay key missing logIndex, and 2 Aderyn High / 5 Slither High+Med findings.

V2 Fix: V2 raises MIN_CALLBACK_GAS_LIMIT to 450,000, keys replay on (txHash, logIndex, ruleId), enforces CEI dispatch, and hits 0 High / 0 Med.

Zero High, Zero Medium Across Our Full Web3-Audit Stack

Every guard in OmniGuard V2 is verified by unit tests, 128,000-call stateful invariants, and dual static analyzers

VERIFIED TOOLCHAIN RESULTS (REPRODUCIBLE LOCALLY IN < 45 SECONDS)

Foundry Unit, Fuzz & Regression	**28 / 28 PASS**	Covers C1, C2, H1, M1, 200ms cooldowns, 256-run conservation fuzz
Foundry Stateful Invariants	**6 / 6 PASS**	256 runs x 128,000 calls, 0 reverts, multi-actor owner/attacker handler
Aderyn v0.6.8 (Cyfrin AST)	**0 High**	Strict CEI + owner-gated coverDebt() (only 5 Low informational items)
Slither v0.11.6 (Trail of Bits)	**0 High, 0 Med**	Zero reentrancy-eth, zero reentrancy-no-eth, zero divide-before-multiply
Gitleaks Secret Scan	**0 Leaks**	Full commit history clean; .env.testnet excluded; fail-closed EIP-712
Dashboard Vitest + Agent Tests	**14 + 5 PASS**	Breaker Lab parity, MLP monotonicity, rule ABI compiler, receipt decoder

6 FORMALLY FUZZED STATEFUL INVARIANTS (OmniGuardInvariants.t.sol)

1. invariant_PortfolioConservationHolds — volatile + stable + debtRepaid == initialTotalAssets always.
2. invariant_AttackerNeverCreatesRulesOrHijacksOwnership — 21,000+ hostile calls result in 0 rules created.
3. invariant_ActiveRuleBucketsStrictlyBounded — active rules/market <= 8, total <= 32 (immune to 900k gas DoS).
4. invariant_CircuitBreakerAndPauseNeverBypassed — 0 callbacks execute while breaker active or vault paused.
5. invariant_TimestampCooldownNeverBypassedByFastBlocks — +200 fast 200ms blocks never double-fire early.
6. invariant_ReceiptCountMatchesGhostExecutions — on-chain receipts.length strictly matches executed callbacks.

Zero-Clone Static Workbench on GitHub Pages

Hosted live at https://alphonshhhomenicmtu.github.io/omniguard-ai/ (HTTP 200, 0 console errors)

Tab 1: Judge Receipt Verifier [ON-CHAIN VERIFIED]

Queries Base Sepolia, Reactive Lasna (rnk_getCommittedSequenceFrontier + IREACT balance + debt), and Unichain Sepolia getReceipt(0..1) live in-browser via viem with clickable BaseScan / Reactscan / Uniscan links.

Tab 2: Adversarial Breaker Lab [SIMULATED V2 MODEL]

6 one-click attack buttons (Unauthorized createRule, Paused Vault, Stale/Duplicate Replay, Flash-Crash Breaker Trip, 200ms Block-Drift, 1h Action Cap Flood) showing exact Solidity custom errors and V1 vs V2 diffs.

Tab 3: Neural & Rule Studio [SIMULATED BROWSER]

Interactive OmniRisk-MLP-7x12x4 stress sliders + plain-English compiler emitting exact V2 createRule() ABI calldata with automatic Base 200ms block-to-timestamp conversion.

Tabs 4 & 5: 60s Walkthrough + /diag [SELF-TEST]

Timed 4-step judge runbook plus live /diag panel verifying all 3 public RPCs, live receipt count >= 2, MLP determinism, and V2 breaker guard parity.

OmniRisk-MLP-7x12x4 & Plain-English Rule Compilation

Transparent engineering: calibrated deterministic weights + cryptographic EIP-712 verification on-chain

NEURAL REGIME CLASSIFIER (7 -> 12 ReLU -> 4 Softmax)

Inputs: price shock magnitude, downside momentum, realized volatility, health-factor stress, cross-chain spread, 60s shock count, and drawdown acceleration. Outputs: CALM / ELEVATED / VOLATILE / CASCADE_CRITICAL, riskScoreBps (0..10000), and recommendedHedgeBps (15%..75%).

Honest disclosure: W1/W2 weights are hand-calibrated deterministic constants (not an opaque externally trained checkpoint) so every browser and Solidity test reproduces the exact same scores.

HOW AI CHANGES ON-CHAIN REACTIVE BEHAVIOR

- CALM: 4.00% drawdown rule stays at 4.00% (0% shift).
- ELEVATED: Tightens drawdown trigger -10% (4.00% -> 3.60%).
- VOLATILE: Tightens -20% (3.20%) & raises HF floor +250 bps.
- CASCADE_CRITICAL: Tightens -35% (2.60%) & boosts hedge up to 75%.
- Proven in Foundry test_NeuralRegime_AdaptiveThresholdTightening:
  -3.0% dip ignored in CALM, fires immediately after CASCADE.

SET IT AND FORGET IT — NATURAL-LANGUAGE TO V2 createRule() CALLDATA

User input: "Hedge 40% of my Base WETH/USDC vault on Unichain if price drops 3.5% with a 15 blocks cooldown"

Safety Warning: Converted "15 blocks" -> 30s strict Unix timestamp cooldown (Base Sepolia 200ms Denim guard).

`Output: kind=STOP_LOSS_HEDGE | action=HEDGE_TO_STABLE | callbackGasLimit=500,000 (>=450k V2 floor) | ABI calldata 0x...`

Zero Solidity required. Strictly validates V2 RuleKind <-> ActionType compatibility before emitting calldata.

Verify Everything in 60 Seconds — Built to Scale to Mainnet

Public workbench, reproducible Foundry + static analysis checks, and concrete path to real ERC-20 per-user vaults

REPRODUCE IN 4 COMMANDS (ZERO TRUST REQUIRED)

```
# 1. Open live public RPC workbench (no clone, no backend, HTTP 200, 0 console errors)
open https://alphonshhhomenicmtu.github.io/omniguard-ai/   # and /diag/ self-test

# 2. Verify live Unichain receipt count directly on public RPC
cast call 0x5b1066a69297e2ec1d1e463741846695 68d3380c "getReceiptsCount()(uint256)" --rpc-url https://sepolia.unichain.org

# 3. Run full V2 Foundry unit + fuzz + 128,000-call stateful invariant suite
cd contracts && forge test -vv

# 4. Confirm 0 High / 0 Medium static analysis & 0 secret leaks
aderyn . && slither . --exclude-dependencies && gitleaks detect --source .. --no-banner
```

NEXT MILESTONES FOR REACTIVE OMNI MAINNET

Phase 1 (Complete): Live Base -> Lasna -> Unichain 2s/3s proofs + V2 security hardening (0 High/0 Med) + Public Judge Workbench.

Phase 2 (Next): Per-user VaultFactory (each user deploys own AbstractCallback vault holding ERC-20 WETH/USDC + Uniswap V4 hook spot feed).

Phase 3 (Mainnet): CRON staleness watchdogs on Reactive Omni Mainnet + split multisig roles (owner / reporter / HSM neural signer).