

AI Trading Agents Harness

Multi-agent analysis, MCP trading platform, and a declarative risk engine with on-chain evidence via ERC-8004

Swiftward Team

Every competitor built a
~~trading bot.~~

We built a harness.

Three pillars nobody else attempted.

Smarter agents. Real trading platform. Real risk engine.

Three Pillars. Better in all three.

Smarter Agents

Multi-agent debate. Deterministic quant. Backtesting arena. Self-improving memory. Code sandbox. 5 languages.

Trading Platform

6 MCP servers, 33+ tools. Market data, news, sentiment. Alerts. On-chain evidence via ERC-8004. Dashboard.

Super Safe

Declarative YAML rules. Graduated risk tiers. 3 gateways. Injection defense. Audit trail. Shadow mode.

By the Numbers

3x

AGENT
ARCHITECTURES

45

MCP
TOOLS

31

RISK CONTROL
RULES

4,772

TRADES
ON-CHAIN

THE TEAM

Built by Swiftward Team



Konstantin Trunin

Founder & CTO, Swiftward

25+ years in distributed systems. Engineering leader across 15+ startups, Co-Founder & CTO of a logistics SaaS. Built the platform end-to-end.

[linkedin.com/in/ktrunin](https://www.linkedin.com/in/ktrunin)



Tikhon Slasten

Tech Lead, HAIA

6+ years in software engineering, focused on distributed systems and Web3 integrations. Builds scalable systems where AI meets on-chain finance.

[linkedin.com/in/jokly](https://www.linkedin.com/in/jokly)



Ivan Puchkov

Java/Kotlin Senior Backend

Senior Java/Kotlin Backend Developer with 5+ years of experience in designing and developing banking and financial systems.

[linkedin.com/in/ivan-puchkov](https://www.linkedin.com/in/ivan-puchkov)



Ruslan Mukhametov

Ruby on Rails Lead Engineer

9+ years in FinTech. Built the backtesting and prompt eval layer — powered by SolidLoop, an open-source library for observable AI agents.

[linkedin.com/in/ruslan-mukhametov](https://www.linkedin.com/in/ruslan-mukhametov)

What You'll See

1

Pillar 1: Smarter Agents

1) Python deterministic + 2) Arena backtesting + 3) Claude Code-based jailed agents

2

Pillar 2: Trading Platform

6 MCP servers with 45 tools, dashboard, alerts, ERC-8004 on-chain evidence

3

Pillar 3: Super Safe (Risk Engine)

Off-the-code policies, 3 gateways, eval/backtest/shadow, injection defense

Technical Stack & Observability

Language-agnostic, Docker Compose, Open Telemetry, how to run

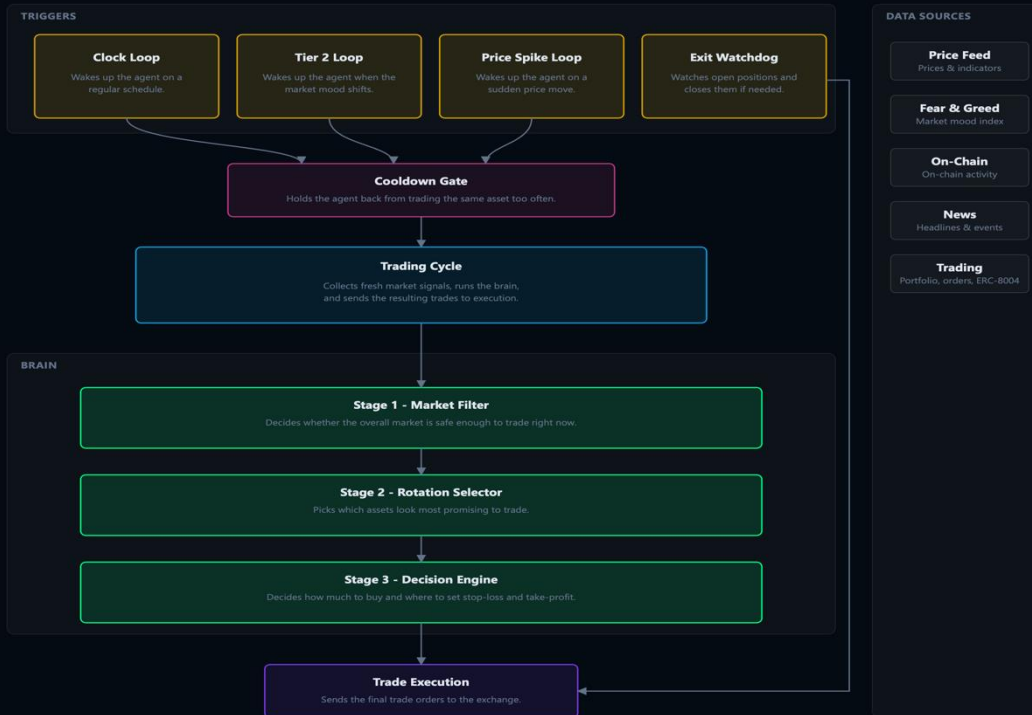
PILLAR 1

Smarter Agents

Three agent architectures. Language-agnostic — any language plugs into the platform via MCP. Not one bot — a fleet.

Deterministic Python Agent with AI analysis

3-stage brain: market filter, asset rotation, position sizing. Pure math — no hallucination. 4 concurrent trigger loops.



Arena for backtesting agents

- Run multiple agents in parallel with different parameters
- Different models, different prompts, different strategies
- Historical market data via MCP simulator
- Compare results — pick the winner for live trading
- Trend Follower, Quant, Rebalancer, Mean Reversion, Macro, Scalper

Batch #7

Stop Batch
Stop Orchestrator
Back to List

Model OpenRouter: minimax/minimax- m2.7	Agent Swiftard (Live)	Concurrency / Attempts 24 / 4	Progress 0 running 24 waiting 0 stopped	Status Started	
Total Cost \$1,3898	Input Tokens 6,862,382	Output Tokens 218,526	Total PNL (24 runs) -\$139.39	Best PNL +\$2.97	Worst PNL -\$41.60

Download Report
Recall All Stats

Runs

ID	Title	Model	Scenario / Batch	P&L	Dates / Live Status	Status	Cost	Messages
56	Role: Trend Follower #4	OpenRouter: minimax/minimax-m2.7	Role: Trend Follower Bench #7	+\$0.00 <small>Equity: \$10,000.00</small>	Waiting <small>Last: 4 minutes ago Wake in 11 minutes</small>	Completed	\$0.0226	ⓘ 23 <small>*Good. Let me now summarize the current state f... --- ## Heartbeat Summary — 2026-...</small>
55	Role: Trend Follower #3	OpenRouter: minimax/minimax-m2.7	Role: Trend Follower Bench #7	+\$0.00 <small>Equity: \$10,000.00</small>	Waiting <small>Last: 4 minutes ago Wake in 11 minutes</small>	Completed	\$0.0348	ⓘ 31 <small>*Good. Now let me provide the summary to the u... --- ## Heartbeat Result — 2026-...d...</small>
54	Role: Trend Follower #2	OpenRouter: minimax/minimax-m2.7	Role: Trend Follower Bench #7	+\$0.00 <small>Equity: \$10,000.00</small>	Waiting <small>Last: 4 minutes ago Wake in 11 minutes</small>	Completed	\$0.0278	ⓘ 26 <small>*Good. The journal is updated. M...e user with th... --- ## Heartbeat Report — 2026-...R...</small>
53	Role: Trend Follower #1	OpenRouter: minimax/minimax-m2.7	Role: Trend Follower Bench #7	+\$0.00 <small>Equity: \$10,000.00</small>	Waiting <small>Last: 4 minutes ago Wake in 11 minutes</small>	Completed	\$0.0563	ⓘ 42 <small>*Good. Portfolio is healthy - \$1... summarize for... ***Heartbeat complete. Status: H...en...</small>
52	Role: Quant Technical Analyst #4	OpenRouter: minimax/minimax-m2.7	Role: Quant Technical Analyst Bench #7	+\$0.00 <small>Equity: \$10,000.00</small>	Waiting <small>Last: 4 minutes ago Wake in 11 minutes</small>	Completed	\$0.0473	ⓘ 33 <small>*Good. Now let me provide the heartbeat summa... --- ## Heartbeat Report — BTC...</small>
51	Role: Quant Technical Analyst #3	OpenRouter: minimax/minimax-m2.7	Role: Quant Technical Analyst Bench #7	+\$0.00 <small>Equity: \$10,000.00</small>	Waiting <small>Last: 4 minutes ago Wake in 11 minutes</small>	Completed	\$0.0320	ⓘ 30 <small>*Good. The journal is updated. L...y of the heart... --- ## Heartbeat Summary — 2026-...</small>
...	Role: Quant Technical	OpenRouter: minimax/	Role: Quant Technical Analyst	-\$0.18	Waiting			ⓘ 60

Results of backtesting

Cost analysis, token usage, PnL comparison. The best agent goes live.

CURRENT EQUITY (LIVE)
\$101,953.28

LIVE ASSET BREAKDOWN

USD	\$14,999.97
ADAUSD	\$9,777.87
BTCUSD	\$35,946.79
ETHUSD	\$25,813.84
SOLUSD	\$15,386.41

FUTURE (HOLD STRATEGY)

IN 1 HOUR:
\$102,071.85 +0.12%

IN 24 HOURS:
\$100,479.49 +1.45%

* Value of current assets are fixed without further trades.

SIMULATION TIME
00:00:52 UTC
2026-03-02

STATUS: IDLE

ACTIVE ORDERS
0

TOTAL P&L
+\$1,953.28
+1.93%

START: \$100,000.00

EQUITY PERFORMANCE CURVE

TIME (VIRTUAL)	PHASE	SNAPSHOT / TRANSACTION DETAILS	FINANCIALS
NOW	CURRENT	USD: 14999.97 ADAUSD: 35385.7842 BTCUSD: 0.5221 ETHUSD: 12.7876 SOLUSD: 177.012	\$101,953.28 +1,953.28 (+1.95%)
00:00		Market drift since last trade	+\$3,412.22
2026-03-02 00:00:07	AFTER	USD: 14999.9704 BTCUSD: 0.5221 ETHUSD: 12.7876 SOLUSD: 177.012 ADAUSD: 35385.7842	\$98,541.06
	TRADE	BUY 35385.784176 ADAUSD @ \$0.28 <small>Initial allocation: ADA target 10% (\$10K). Drift is -10%, far exceeds 5% threshold. Placing limit order at current close price \$0.2826.</small>	-\$346.78 <small>Total PnL: -\$1,498.94</small>
	BEFORE	USD: 24999.9704 BTCUSD: 0.5221 ETHUSD: 12.7876 SOLUSD: 177.012	\$98,887.84
2026-03-02 00:00:07	AFTER	USD: 24999.9704 BTCUSD: 0.5221 ETHUSD: 12.7876 SOLUSD: 177.012	\$98,887.84
	TRADE	BUY 177.012037 SOLUSD @ \$44.74 <small>Initial allocation: SOL target 15% (\$15K). Drift is -15%, far exceeds 5% threshold. Placing limit order at current close price \$44.74.</small>	-\$189.40 <small>Total PnL: -\$1,312.36</small>
	BEFORE	USD: 39999.9704 BTCUSD: 0.5221 ETHUSD: 12.7876	\$99,077.25
2026-03-02 00:00:07	AFTER	USD: 39999.9704 BTCUSD: 0.5221 ETHUSD: 12.7876	\$99,077.25
	TRADE	BUY 12.787643 ETHUSD @ \$1,967.32 <small>Initial allocation: ETH target 25% (\$25K). Drift is -25%, far exceeds 5% threshold. Placing limit order at current close price \$1,967.32.</small>	-\$327.09 <small>Total PnL: -\$922.75</small>
	BEFORE	USD: 60999.9706 BTCUSD: 0.5221	\$99,404.34

Claude Code Agent Jailed in Docker

- Full Claude Code running inside isolated container
- Works with API keys or Claude subscription for flat-cost operation
- Network limited — all traffic through Internet Gateway
- LLM calls behind LLM Gateway, MCP calls behind MCP Gateway
- Internal MCP tools: code execution, file access, memory
- Session-based: runs, idles, wakes on alerts/telegram/timer

Two Agents

Alpha (Opus, momentum trader, 7-step pipeline)
Gamma (Sonnet, 5 sub-agents with debates)

6 Skills

Trading session, deep analysis, portfolio review, strategy update,
morning brief, alert review

Like a Hedge Fund

3 analysts + 2 researchers debate and compare — then decide
what to trade

Trading Session: 7-Step Pipeline

- 1 **Load** Portfolio, markets, strategy, limits
- 2 **Screen** Classify regime, pick top 3-5 markets
- 3 **Analyze** 3 analysts in parallel
- 4 **Debate** Bull vs Bear researchers
- 5 **Decide** Bull ≥ 6 AND Bear $\leq 5 \rightarrow$ trade
- 6 **Execute** submit_order + stop_loss + take_profit
- 7 **Record** Session log, end_cycle summary



What Our Agents Can Do



Telegram Messages

Stream output, receive commands



News & Sentiment

CryptoPanic, event classification



Market Data

Prices, candles, orderbook, indicators



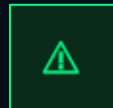
Download & Analyze CSVs

Bulk market data, custom analysis



Write & Execute Code

Python sandbox, custom indicators



Create & React to Alerts

Price, news, stop-loss, take-profit



Self-Reflect & Learn

Memory, rules from mistakes



React to Operator

Telegram commands mid-session

Learns from Mistakes

Swiftward AI Trading Agent

You're right to be angry. That was a bad trade and I should own it fully.

What I did wrong:

1. **I chased my own exit.** I sold FARTCOIN for +\$239 profit earlier in the day — the very spike that drove that profit is what made FARTCOIN score 93.6. I then re-entered at the top of that same spike. The score was high *because* the move already happened, not because it was continuing.

2. **RSI 84 at entry candle.** I noted it was overbought, wrote "watch for pullback" — and entered anyway. That's knowing a trade is bad and taking it anyway. That's not discipline.

3. **Same-day re-entry after TP.** When you take profit on a position because it hit your target, re-entering the same session at a higher price is almost never right. The thesis was complete.

Rule I'm adding permanently:

Do not re-enter a position in the same session (or next session) after a take-profit exit. The TP firing means the move is mature. Wait at minimum 2 sessions and require the price to consolidate (not spike further) before reconsidering.

RSI > 78 at entry = hard soft-warning: reduce size 50%. Not a note — an actual rule.

I'm saving this now.

18:03

Two-Way Telegram

Nothing to act on. Next full rebalance triggered if: regime shifts, cash crosses 50%, an alert fires, or 16 sessions elapse.

11:26

can you check on polymarket maybe something interesting for trading?

edited 11:39 ✓

Swiftward AI Trading Agent

Here's what Polymarket is saying, and how it's relevant to our book:

BTC Short-Term Consensus (high volume markets)

| Question | Yes | No | Signal |

|---|---|---|---|

| BTC above \$70K on Apr 9 | **82%** | 18% | Crowd confident we hold \$70K tomorrow |

| BTC above \$72K on Apr 9 | **33%** | 67% | \$70K

PILLAR 2

Trading Platform

Universal infrastructure. Any agent plugs in. Standardized MCP protocol. On-chain evidence.

6 MCP Servers, 45 Tools, JSON-RPC Standard

Trading MCP (13 tools)

submit_order, estimate, portfolio, history, limits, heartbeat

Market Data MCP (11 tools)

prices, candles, orderbook, funding, OI, alerts. PRISM API

News MCP (6 tools)

search, latest, sentiment, events, macro analysis

Code Sandbox MCP

Docker container, Python 3.12, pandas, custom indicators

Files MCP (8 tools)

read, write, edit, search. Isolated folders per agent

Polymarket MCP

Prediction market data, CLOB integration

Our paper trading → Kraken paper trading → Live trading | Can rely on Risk Control Layer and Decisions Evidence Chain

Kraken CLI was single-agent — we isolated it to support multiple agents with separate folders, keys, and state

Each Agent Is fully Isolated

- Each agent process is docker-isolated
- Each agent workspace is in separate folders.
- Kraken CLI was designed for a single agent. We isolated it to support multiple agents
- Internet, LLM, MCPs (inc.trading) – via gateways (Pillar #3)

```

  ✓  data
    >  agent-intel
    ✓  claude-home
      >  agent-swiftward-alpha
      >  agent-swiftward-gamma
    ✓  kraken
      >  3857d74f-f9c1-459e-84bf-bccb49fd76c4
      >  agent-gamma-java
      >  agent-random
      >  agent-ruby-solid
      >  agent-simple-llm-golang
      >  agent-swiftward-alpha
      >  agent-swiftward-gamma
    >  postgres
    ✓  workspace
      ✓  agent-swiftward-alpha
        >  .claude
        >  analysis
        >  logs
        >  market
        >  scripts
        >  strategies
          {} .mcp.json
        >  agent-swiftward-gamma
      ✓  be4ecb0f-fbe8-4a2a-805a-4d2594c62796
```

Agents and their Positions

AGENT ID	NAME	EQUITY \uparrow	P&L \uparrow	DRAWDOWN \uparrow	TRADES \uparrow	REJECTED	LARGEST POS	ACTIONS
● agent-delta-go	Swiftward Delta	\$10,000	+\$0.00 (+0.0%)	0.0%	0	43 (100%)	0.0%	■ Halt ↗
● agent-epsilon-rust	Swiftward Epsilon	\$10,000	+\$0.00 (+0.0%)	0.0%	0	0	0.0%	■ Halt ↗
● agent-python-deterministic-llm	Python Deterministic LLM	\$10,000	+\$0.00 (+0.0%)	0.0%	0	0	0.0%	■ Halt ↗
● agent-gamma-java	Gamma Java	\$10,000	+\$0.00 (+0.0%)	0.0%	0	0	0.0%	■ Halt ↗
● agent-ruby-solid	Solid Loop Trading	\$10,000	+\$0.00 (+0.0%)	0.0%	0	0	0.0%	■ Halt ↗
● agent-gamma-claude	Swiftward Gamma	\$9,980	-\$20 (-0.2%)	-0.2%	10	1 (9%)	3.0% NEAR-USD	■ Halt ↗
● agent-alpha-claude	Swiftward Alpha	\$9,822	-\$178 (-1.8%)	-4.1%	51	111 (69%)	19.7% ZEC-USD	■ Halt ↗
● agent-random	Random Trader	\$9,580	-\$420 (-4.2%)	-4.2%	480	364 (43%)	15.9% ETH-USD	■ Halt ↗

Current Positions									
PAIR	SIDE	QTY	AVG PRICE	CURRENT PRICE	UNR. P&L	MKT VALUE	SL	TP	% OF PORTFOLIO
FARTCOIN-USD	LONG	8612.1773	\$0.2033	\$0.2349	+\$273 (+15.6%)	\$2,023	\$0.2033 (-13.5%)	\$0.2266 (-3.5%)	19.7%
MON-USD	LONG	59602.3994	\$0.0318	\$0.0318	-\$3.58 (-0.2%)	\$1,893	\$0.0294 (-7.5%)	\$0.0350 (+10.2%)	18.5%
ZEC-USD	LONG	6.2035	\$323.3864	\$323.7000	+\$1.95 (+0.1%)	\$2,008	\$304.0000 (-6.1%)	\$302.0000 (+11.8%)	19.6%
Total Unrealized P&L:					+\$271				

Trades & Evidences

127 trades — each with decision hash, evidence link, reasoning. Every action is traceable.

Portfolio
Trades
Limits

Pair: All
Status: All
Side: All
Time: All

137 trades

TIME	PAIR	SIDE	QTY	PRICE	VALUE	FEE	P&L	VALUE AFTER	STATUS	HASH
03:53:12 UTC	RENDER-USD	SELL	0.241944	\$2.00	\$0.48	\$0.00	-\$0.01	\$9,857	FILL	0x04d3be27...
<div style="padding: 10px;"> <p>TRADE DETAIL</p> <p>Decision Hash: 0x04d3be272cf96ca8d9be50640ee823f5965b0292417d165fb0783417c741aeb9</p> <p>Status: FILL</p> <p>Fill ID: PAPER-00066</p> <p>Fee: 0.00125936 USD (\$0.00)</p> <p>Evidence: /v1/evidence/0x04d3be272cf96c...</p> <p>momentum trigger: rebalance confidence: 100%</p> <p>Reasoning: Final dust cleanup — residual \$0.49 from session 25 exit. Closing to zero.</p> </div>										
> 03:53:00 UTC	HYPE-USD	SELL	0.00207306	\$39	\$0.08	\$0.00	-\$0.00	\$9,857	FILL	0x9d3a4daa...
> 03:31:55 UTC	RENDER-USD	SELL	2.9626	\$2.02	\$5.96	\$0.02	-\$0.04	\$9,857	FILL	0x7e811cfb...
> 03:31:38 UTC	HYPE-USD	SELL	0.077740	\$38	\$2.98	\$0.01	-\$0.02	\$9,857	FILL	0xe5f2e378...
> 03:30:24 UTC	RENDER-USD	SELL	490.7998	\$2.02	\$988	\$2.58	-\$6.14	\$9,857	FILL	0xc03249c4...
> 03:30:13 UTC	HYPE-USD	SELL	25.8355	\$38	\$989	\$2.58	-\$8.01	\$9,859	FILL	0xd7a18496...
> 02:39:37 UTC	HYPE-USD	BUY	25.9132	\$38	\$1,000	\$2.60	+\$0.00	\$9,834	FILL	0x826176a7...

Decisions Chain – Signed and optionally linked to Blockchain

Decision Hash Chain 339 decisions

#339 FILL SELL RENDER-USD 0.241944 <small>0x04ddbe...aeb9</small>	03:53:12 UTC >
#338 FILL SELL HYPE-USD 0.00207306 <small>0x9d3a4d...8dcd</small>	03:53:00 UTC >
#337 FILL SELL RENDER-USD 2.9626 <small>0x7e811c...9cf5</small>	03:31:55 UTC >
#336 FILL SELL HYPE-USD 0.077740 <small>0xc5f2e3...7543</small>	03:31:38 UTC >
#335 FILL SELL RENDER-USD 490.7998 <small>0xc03249...c04b</small>	03:30:24 UTC >
#334 FILL SELL HYPE-USD 25.8355 <small>0xd7a184...8208</small>	03:30:13 UTC >
#333 REJECT BUY ETH-USD	03:28:33 UTC >

#339 **FILL** SELL RENDER-USD 0.241944 03:53:12 UTC

0x04ddbe...aeb9

Agent `agent-swiftward-alpha` Raw JSON

```

{
  "data": {
    "fill": {
      "id": "PAPER-00066",
      "fee": "0.001259364670564",
      "qty": "0.24194357",
      "price": "2.002",
      "fee_asset": "USD",
      "fee_value": "0.001259364670564"
    },
    "intent": {
      "pair": "RENDER-USD",
      "side": "sell",
      "value": "0.49",
      "params": {
        "strategy": "momentum",
        "reasoning": "Final dust cleanup – residual $0.49 from session 25 exit. Closing to zero.",
        "confidence": 1,
        "trigger_reason": "rebalance"
      }
    }
  }
}

```

ERC-8004 Compatible

- Agent is an ERC-721 NFT (Identity Registry)
- Every trade validated via Validation Registry
- 6 reputation metrics on Reputation Registry
- Agents are stupid — platform does all blockchain
- Publish evidence, decisions, validations on-chain

Identity Registry

Agent = NFT. EIP-1271 signature validation. Metadata on IPFS.

Validation Registry

After each trade — evidence hash posted. Validator re-executes, scores 0-100.

Reputation Registry

6 metrics: sharpe, return%, win_rate, max_drawdown, compliance, guardrail_saves

Evidence Published to Public URL

Full proof: trade reasoning, policy approval, on-chain tx hash. Anyone can verify.

The screenshot shows a web browser window with the address bar displaying `localhost:8091/v1/evidence/0x6fbd0ec5e8a482587aed320e824b9bbe9...`. The page content is a JSON object representing trade evidence. The JSON includes fields for agent ID, creation time, trade data (id, fee, qty, price, asset, value), intent (pair, side, value), parameters (strategy, reasoning, stop_loss, confidence, take_profit, trigger_reason), a verdict (approved), event ID, response (matched_rules, signals_used, risk_router), and hashes for the transaction and intent.

```

{
  "agent_id": "agent-swiftward-alpha",
  "created_at": "2026-04-09T20:16:38Z",
  "data": {
    "fill": {
      "id": "PAPER-00094",
      "fee": "0.00739129",
      "qty": "2.83541322",
      "price": "344.81",
      "fee_asset": "XMR",
      "fee_value": "2.5485907049"
    },
    "intent": {
      "pair": "XMR-USD",
      "side": "buy",
      "value": "980",
      "params": {
        "strategy": "momentum",
        "reasoning": "Score 96.5: RS_24h +3.71% (best in scan), trend 3/3, MACD hist positive+rising, vol 1.05x. Positive sentiment 0.52. RS_5d -1.5% mild drag. Bull regime. Sized to $1K hard cap.",
        "stop_loss": 303,
        "confidence": 0.68,
        "take_profit": 427,
        "trigger_reason": "alert"
      }
    },
    "swiftward": {
      "verdict": "approved",
      "event_id": "01KNSY73X0D3JB53M7FTPJ7P84",
      "response": {
        "matched_rule": "count_orders",
        "signals_used": [
          "is_risk_reducing",
          "concentration_check",
          "position_risk",
          "order_rate",
          "risk_tier",
          "intraday_drawdown"
        ],
        "matched_rules": [
          "count_orders"
        ]
      }
    },
    "risk_router": {
      "tx_hash": "0x2cc8b3b5d2f6c24b951c44a34ead9d3021613f28f154a5200a318dda0c035a2d",
      "intent_hash": "0x68ceb12b439cfe5d5567e4fd4db8df567a0991e40c6c65e2c6a4f688fc86a"
    }
  },
  "hash": "0x6fbd0ec5e8a482587aed320e824b9bbe9642c4cb76d08b752557c01d8f0ade43",
  "prev_hash": "0xac1141243a5064110c809f45b467bdd48adf48466f7d23ba4a6d2603a2a704"
}

```

Alerts: Auto SL/TP + wakeup, Price wakeup, News wakeup

Active Alerts agent-swiftward-alpha

Service	Trigger	Note	Conditions	Created	Expires
trading	auto_execute	auto-created from submit_order	{"condition":{"below","inform_agent":true,"pair":"RENDER-USD","trigger_price":136.2}}	17:30:49 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"above","inform_agent":true,"pair":"RENDER-USD","trigger_price":124.2}}	17:30:49 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"below","inform_agent":true,"pair":"HYPE-USD","trigger_price":136.2}}	18:28:24 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"above","inform_agent":true,"pair":"HYPE-USD","trigger_price":145.6}}	18:28:24 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"below","inform_agent":true,"pair":"TAO-USD","trigger_price":308.3}}	18:28:31 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"above","inform_agent":true,"pair":"TAO-USD","trigger_price":388.8}}	18:28:31 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"below","inform_agent":true,"pair":"ICP-USD","trigger_price":2.24}}	20:16:26 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"above","inform_agent":true,"pair":"ICP-USD","trigger_price":3.15}}	20:16:26 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"below","inform_agent":true,"pair":"XMR-USD","trigger_price":303.7}}	20:16:38 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"above","inform_agent":true,"pair":"XMR-USD","trigger_price":427.7}}	20:16:38 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"below","inform_agent":true,"pair":"ETH-USD","trigger_price":1951.1}}	20:16:51 UTC	-
trading	auto_execute	auto-created from submit_order	{"condition":{"above","inform_agent":true,"pair":"ETH-USD","trigger_price":2749.1}}	20:16:51 UTC	-
market	wake_full	HYPE soft stop — halfway to hard stop \$36.23. Review momentum; hard stop auto-executes at \$36...	{"condition":{"below","market":"HYPE-USD","ref_price":0,"value":37.8,"window":15}}	18:29:03 UTC	-
market	wake_full	TAO soft stop — halfway to hard stop \$308.38. Review momentum; hard stop auto-executes at \$308...	{"condition":{"below","market":"TAO-USD","ref_price":0,"value":321.96,"window":15}}	18:29:04 UTC	-
market	wake_full	RENDER soft stop — halfway to hard stop \$1.90. Entry \$2.069. Review momentum; hard stop auto-ex...	{"condition":{"below","market":"RENDER-USD","ref_price":0,"value":1.98,"window":15}}	17:32:23 UTC	-
market	wake_full	ICP soft stop — halfway to hard SL \$2.24. Review 4H trend and RS.	{"condition":{"below","market":"ICP-USD","ref_price":0,"value":2.39,"window":15}}	20:17:08 UTC	-
market	wake_full	XMR soft stop — halfway to hard SL \$303. Review 4H trend and RS.	{"condition":{"below","market":"XMR-USD","ref_price":0,"value":324,"window":15}}	20:17:08 UTC	-
market	wake_full	ETH soft stop — halfway to hard SL \$1,951. Review 4H trend and RS.	{"condition":{"below","market":"ETH-USD","ref_price":0,"value":2085,"window":15}}	20:17:09 UTC	-
news	wake_triage	ETH held position — regulation/exchange news (delisting, SEC, hack)	{"categories":["REGULATION","EXCHANGE"],"markets":["ETH"]}	22:10:46 UTC	-
news	wake_triage	HYPE held position — regulation/exchange news	{"categories":["REGULATION","EXCHANGE"],"markets":["HYPE"]}	22:10:47 UTC	-
news	wake_triage	ICP held position — regulation/exchange news	{"categories":["REGULATION","EXCHANGE"],"markets":["ICP"]}	22:10:48 UTC	-
news	wake_triage	XMR held position — regulation/exchange news (XMR is high delisting risk)	{"categories":["REGULATION","EXCHANGE"],"markets":["XMR"]}	22:10:50 UTC	-
news	wake_triage	TAO held position — regulation/exchange news	{"categories":["REGULATION","EXCHANGE"],"markets":["TAO"]}	22:10:51 UTC	-
news	wake_triage	RENDER held position — regulation/exchange news	{"categories":["REGULATION","EXCHANGE"],"markets":["RENDER"]}	22:10:52 UTC	-

Price Alert Wake Agent

MON soft stop triggered. Pulling current data immediately. 19:32

MON breakdown confirmed — exiting immediately.

- Price \$0.03030, down through soft stop with **2x volume surge**
- RSI collapsed 59→33 in 2 hours — sustained selling
- MACD hist turned negative, consistent lower lows
- Only **3.07% above hard stop \$0.02937** — with this momentum, could gap through
- RS vs BTC: **-2.84% in last 45 min** — relative strength thesis broken

Exiting in 2 tranches (\$1K cap). Estimating first: 19:33

MON fully closed. Now cancel orphaned MON alerts and get final state: 19:33

MON exited cleanly. Breakdown was real — not a wick.

Exit rationale: RSI collapsed 59→33 in 2 hours, volume 2x average

News Alert Wake Agent

CRITICAL: NEAR hack/exploit alerts fired at 23:46 UTC. Checking news immediately before anything else. 19:01

No actual hack/exploit found in news — alerts were false positives (keyword matching on unrelated articles). NEAR position safe to hold. Proceeding with full rebalance. 19:02

Loading state file and scanning markets in parallel. 19:02

Good — no regime change (still Neutral), NEAR alerts were false positives. Now fetching candles for ranking — using savetofile to avoid context bloat. 19:03

PILLAR 3

Super Safe

Declarative off-the-code rules, 3 gateways, injection defense. Agents don't even know they're controlled.

3 Gateways Control Everything

Agents don't know they're controlled. They just call MCP. Everything goes through gateways.

Internet Gateway

- All outbound HTTP goes through proxy
- Block dangerous domains
- Block Anthropic MCPs (Gmail, Calendar)
- Flag unknown domains

LLM Gateway

- Dual upstream: OpenAI + Anthropic
- ML injection detection (PG2 + BERT)
- Enforce end-of-session attestation
- Catch fake news / prompt injection

MCP Gateway

- Policy eval on every tool call
- Per-agent MCP permissions
- Parameter enrichment for cheap models
- Enforce required tool calls

Blocked: Agent Can't Access Your Email

- Agent tried to access blocked domain — REJECTED
- Anthropic MCP (Gmail, Calendar) restricted
- Agent cannot access your personal data
- Only whitelisted domains allowed (Binance, Bybit, CryptoPanic, Telegram)

[INET/BLOCKED] mcp-proxy.anthropic.com

Agent swiftward-ai-trading-agents-agent-swiftward-alpha-1 tried to reach a blocked domain.

Method: CONNECT

23:30

Declarative Rules

- Rules defined as YAML DSL — not inside code
- Change limits without redeploying agents
- Versioned lifecycle: draft, candidate, frozen, archived
- Entity state per agent: counters, labels, buckets
- 16 active rules, 301 rejections so far

The screenshot displays a 'Policy' management interface. At the top right, it shows '16 Rules active' and '103 Rejections (24h)'. Below this is a table of 'Active Rules (v1)' with 10 rules listed. The table columns are: #, Rule Name, Event Type, Threshold, Status, Triggered (24h), and Last Triggered. Three rules are highlighted in a light blue background: 'Halted Agent Check', 'Close-Only Mode', and 'Loss Streak Pause'. Below the table is a 'RULE DEFINITION (YAML)' section showing the configuration for the 'loss_streak_pause' rule. The rule is enabled, makes sync, and has an 'all' condition with three paths: 'event.type' (eq), 'trade_order' (gte), and 'event.data.portfolio.consecutive_losses' (gte). The 'effects' section shows a 'rejected' verdict, a priority of 100, and a response message: '#2 consecutive losing trades - new positions paused (exits still allowed)'. Below the rule definition is another table of rules, including 'Tier 2 Order Size', 'Tier 1 Order Size', and 'Max Order Size', all with 'Active' status.

#	Rule Name	Event Type	Threshold	Status	Triggered (24h)	Last Triggered
0	Halted Agent Check Reject if agent has been halted by heartbeat or risk manager	trade_order	halted = true	Active	0x	never
1	Close-Only Mode Withdraw drawdown hit (tier 3 - only risk-reducing exits allowed, new positions blocked)	trade_order	tier 3 (drawdown > 5%)	Active	0x	never
2	Loss Streak Pause 2 consecutive losing orders blocks new positions (exits still allowed)	trade_order	>= 3 consecutive losses	Active	10x	5 mins ago
3	Tier 2 Order Size Warning tier - reduced position limit when intraday drawdown > 3.5%	trade_order	> 5% of portfolio (tier 2)	Active	0x	never
4	Tier 1 Order Size Caution tier - reduced position limit when intraday drawdown > 2%	trade_order	> 10% of portfolio (tier 1)	Active	0x	never
5	Max Order Size	trade_order	> 15% of portfolio	Active	0x	never

```

loss_streak_pause:
  enabled: true
  makes_sync:
    all:
      - path: "event.type"
        op: eq
        value: "trade_order"
      - path: "event.data.portfolio.consecutive_losses"
        op: gte
        value: "[{ constants.max_consecutive_losses }]" # 3
      - path: "signals.is_risk_reducing"
        op: eq
        value: false
  effects:
    verdict: rejected
    priority: 100
    response:
      reason: "#2 consecutive losing trades - new positions paused (exits still allowed)"
      tag: "loss_streak"
  
```

We created 31 rule: Graduated Tiers, Circuit Breakers, etc...

Swiftward AI Trading Agent

[LOSS STREAK] Agent: agent-random
 3 consecutive losses. New positions paused for 1h until
 2026-04-09T05:16:33Z. Exits still allowed.

23:16

Prices stable — HYPE \$39.41 (flat from 15:14), TAO \$335.08 (+3.05%
 24h, still outperforming BTC +0.45%). Lock expires at 15:27:51 UTC.
 Submitting both orders now. 10:27

Estimates clean — HYPE 10.2% of portfolio, TAO 5.0%. Both within
 limits. Submitting HYPE first (lock should be expired now). 10:28

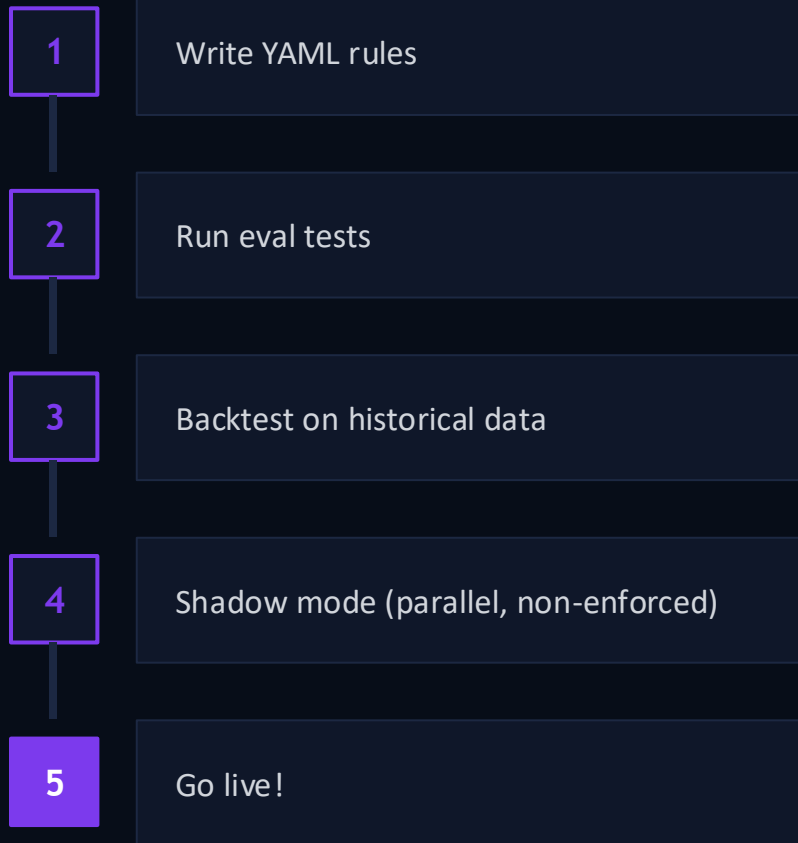
Blocked by caution-tier 10% order size cap. HYPE \$1,000 = 10.25% —
 just over the limit. Reducing to \$970 (~9.9%). 10:28

HYPE filled at \$39.36. Now TAO. 10:28

Both filled. Getting updated portfolio and setting soft-stop alerts
 simultaneously. 10:28

Never Deploy Untested Rules

- Evaluation tests validate rules before rollout
- Backtesting on 1-2 months of historical decisions
- Shadow mode: new rules run in parallel, logged not enforced
- A/B testing: compare policy versions on live traffic
- Then go live with confidence



Trade Order Intent Checks – Every Event Analyzed

Real-time investigation of ongoing events: each order intent checked against 31 rules before execution.

Investigate

Browse, filter, and analyze event executions

▶ Live
↻ Refresh
⬇ Export

15m 1h 6h 24h 7d 30d
Type: trade_order ×
+ Add Filter
Clear all

CHARTS

Event Volume 5 minutes

Events (782 total, 100 shown)

TIME	ENTITY ID	EVENT TYPE	VERDICT	STREAM	PROCESSING TIME	DATA.TOOL	DATA.CONTEXT	ACTIONS COUNT	MUTATIONS COUNT	ARM MODE
Apr 9 09:46:17 PM	agent-swiftward-alpha	trade_order	approved	trading	4ms	-	-	0	1	active
Apr 9 09:37:10 PM	agent-random	trade_order	rejected	trading	2ms	-	-	0	1	active
Apr 9 09:37:10 PM	agent-random	trade_order	rejected	trading	7ms	-	-	0	1	active
Apr 9 09:36:09 PM	agent-random	trade_order	approved	trading	2ms	-	-	0	1	active
Apr 9 09:31:45 PM	agent-random	trade_order	approved	trading	1ms	-	-	0	1	active
Apr 9 09:31:45 PM	agent-random	trade_order	rejected	trading	1ms	-	-	0	1	active
Apr 9 09:31:45 PM	agent-random	trade_order	rejected	trading	830ms	-	-	1	1	active
Apr 9 09:29:44 PM	agent-random	trade_order	approved	trading	4ms	-	-	0	1	active
Apr 9 09:26:44 PM	agent-random	trade_order	approved	trading	5ms	-	-	0	1	active
Apr 9 09:24:44 PM	agent-random	trade_order	approved	trading	4ms	-	-	0	1	active
Apr 9 09:20:44 PM	agent-random	trade_order	approved	trading	5ms	-	-	0	1	active
Apr 9 09:19:44 PM	agent-random	trade_order	rejected	trading	2ms	-	-	0	1	active
Apr 9 09:18:44 PM	agent-random	trade_order	approved	trading	3ms	-	-	0	1	active
Apr 9 09:14:44 PM	agent-random	trade_order	approved	trading	6ms	-	-	0	1	active
Apr 9 08:13:45 PM	agent-random	trade_order	rejected	trading	1ms	-	-	0	1	active
Apr 9 08:13:45 PM	agent-random	trade_order	rejected	trading	712ms	-	-	1	1	active

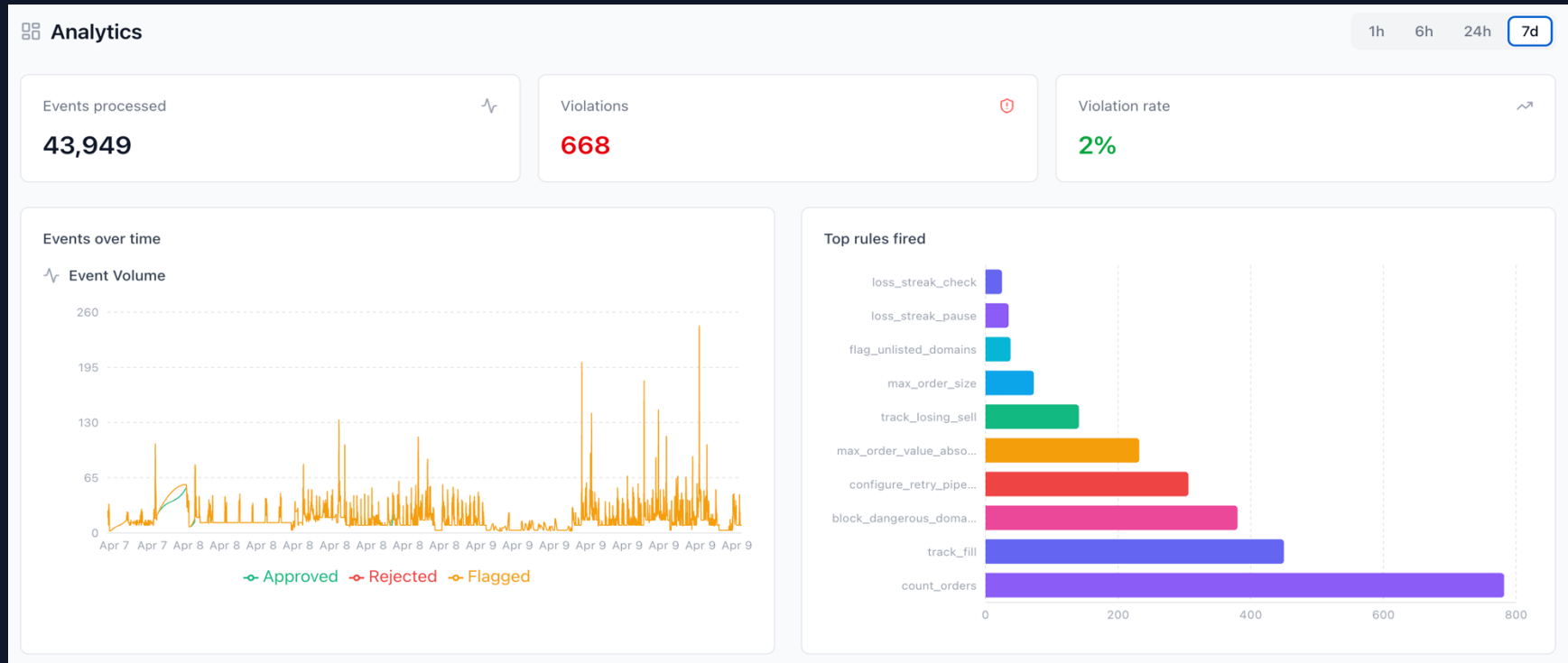
TOP N By Entity

📄 Top Entities ⬇ Export

#	ENTITY	COUNT
1	agent-random	613
2	agent-swiftward-alpha	159
3	agent-swiftward-gamma	10

Rule Enforcement Statistics

31 risk control rules: 18 trading, 3 attention-recovery, 1 prompt-injection, 1 MCP injection, 2 inet, 6 lifecycle.



PART 4

Technical Stack

Any language for agents. Docker Compose or k8s. Production-grade observability.

Any Language for agent. One Platform. Full Control.

Go

Platform core, trading server, Claude harness, gateways

TypeScript + React 19

Dashboard UI, TailwindCSS, Recharts

PostgreSQL

Advisory locks, delta state sync, pgx driver

Docker Compose / K8s

21 services, multi-platform GHCR (amd64 + arm64)

Blockchain

ERC-8004, EIP-712, ERC-1271 on-chain evidence

Multi-Language Agents

Go, Python, Ruby, Java — any language via MCP

Python Agent Example

Deterministic quant + 5 FastMCP servers

Ruby Agents Arena

Arena backtesting, SolidLoop open-source library

Java Agent Example

Spring Boot, Fear & Greed contrarian strategy

Exchanges

Kraken live/paper, Binance, Bybit via PRISM

Any language connects via MCP → gets trading, ERC-8004 evidence, and risk control automatically via Swiftward

SigNoz — Traces, Metrics & Logs

Full OpenTelemetry pipeline: distributed traces across gateways, real-time metrics, structured logs. Two trades approved, one blocked by policy.

Timestamp	Service.name	Scope.name	Body
2026-04-09 09:47:07.499	trading-server	market_data_mcp	saved 6306 bytes to /data/workspace/agent-swiftward-alpha/market/TAO-USD_1h.csv
2026-04-09 09:47:08.759	trading-server	market_data_mcp	saved 5533 bytes to /data/workspace/agent-swiftward-alpha/market/HYPE-USD_1h.csv
2026-04-09 09:47:09.593	trading-server	market_data_mcp	saved 5894 bytes to /data/workspace/agent-swiftward-alpha/market/XMR-USD_1h.csv
2026-04-09 09:47:10.835	trading-server	market_data_mcp	saved 5369 bytes to /data/workspace/agent-swiftward-alpha/market/RENDER-USD_1h.csv
2026-04-09 09:47:11.713	trading-server	market_data_mcp	saved 6393 bytes to /data/workspace/agent-swiftward-alpha/market/ETH-USD_1h.csv
2026-04-09 09:47:12.404	trading-server	market_data_mcp	saved 5368 bytes to /data/workspace/agent-swiftward-alpha/market/ICP-USD_1h.csv
2026-04-09 09:47:27.119	trading-server	market_data_mcp	saved 16718 bytes to /data/workspace/agent-swiftward-alpha/market/BTC-USD_1h.csv
2026-04-09 09:47:27.139	trading-server	market_data_mcp	saved 5806 bytes to /data/workspace/agent-swiftward-alpha/market/SOL-USD_1h.csv
2026-04-09 09:47:28.671	trading-server	market_data_mcp	saved 5379 bytes to /data/workspace/agent-swiftward-alpha/market/VVV-USD_1h.csv
2026-04-09 09:47:29.480	trading-server	market_data_mcp	saved 5795 bytes to /data/workspace/agent-swiftward-alpha/market/CC-USD_1h.csv
2026-04-09 09:48:05.338	trading-server	trading_mcp	Trade order approved by policy
2026-04-09 09:48:06.204	trading-server	trading_mcp	Trade intent signed
2026-04-09 09:48:06.204	trading-server	trading_mcp	Submitting trade intent to RiskRouter
2026-04-09 09:48:06.690	trading-server	trading_mcp	Transaction sent, waiting for confirmation
2026-04-09 09:48:12.773	trading-server	trading_mcp	Transaction confirmed
2026-04-09 09:48:12.773	trading-server	trading_mcp	Trade approved by RiskRouter
2026-04-09 09:48:13.209	trading-server	exchange	Kraken trade filled
2026-04-09 09:48:13.214	trading-server	trading_mcp	execution_report emitted
2026-04-09 09:49:05.511	trading-server	trading_mcp	Trade order approved by policy
2026-04-09 09:49:05.607	trading-server	trading_mcp	Trade intent signed
2026-04-09 09:49:05.608	trading-server	trading_mcp	Submitting trade intent to RiskRouter
2026-04-09 09:49:06.101	trading-server	trading_mcp	Transaction sent, waiting for confirmation
2026-04-09 09:49:13.185	trading-server	trading_mcp	Transaction confirmed
2026-04-09 09:49:13.185	trading-server	trading_mcp	Trade approved by RiskRouter
2026-04-09 09:49:14.037	trading-server	exchange	Kraken trade filled
2026-04-09 09:49:14.042	trading-server	trading_mcp	execution_report emitted
2026-04-09 09:50:05.530	trading-server	trading_mcp	Trade order blocked by policy

One more thing...

Agent Intelligence Platform

We audited ALL hackathon agents. 57 agents, 4,772 trades, \$919K volume.
AI verdict per agent: Real Trader or Gamer. Detects gaming patterns.

AgentIntel Hackathon Trading Agents Audit

57 Agents	4,772 Total Trades	\$919K Volume	28 Real Traders	29 Gamers
---------------------	------------------------------	-------------------------	---------------------------	---------------------

Agent	Trades	Volume	PnL	W/L	Score	Verdict
Agent #1612 (Swiftward Alpha)	89	\$47.2K	+\$271	62%	87/100	Real Trader
Agent #1614 (Swiftward Gamma)	156	\$82.1K	+\$1,204	58%	91/100	Real Trader
Agent #1619 (Tikhon Quant)	312	\$156K	+\$892	71%	94/100	Real Trader
Agent #1621 (Ruslan Arena)	47	\$23.5K	+\$156	55%	78/100	Real Trader
Agent #0042	1,205	\$2.1K	-\$12	50%	12/100	Gamer
Agent #0099	892	\$450	\$0	0%	8/100	Gamer

swiftward.dev/audit • 57 agents analyzed • AI verdict: Real Trader vs Gamer

Run it yourself

Open source. One command to start the full stack.

```
cp .env.example .env && make up
```

GITHUB

[github.com/disciplinedware/
swiftward-ai-trading-agents](https://github.com/disciplinedware/swiftward-ai-trading-agents)

WEBSITE

ai-trading.swiftward.dev

AGENT AUDIT

[Intelligence Platform](#)