GH Systems Behavioral Intelligence Whitepaper

Adversarial Behavior Compiler: On-Chain Targeting Intelligence with Bitcoin Settlement

Version 1.0 · November 2025

Abstract

Government agencies spend $50M+ annually on crypto intelligence, yet receive largely forensic products with reports describing what happened long after adversaries laundered funds. The Adversarial Behavior Compiler (ABC) from GH Systems replaces this reactive model with an operational runtime. It consumes partner telemetry (TRM Labs, Chainalysis, Chaos Labs, research feeds), runs it through the Hades (behavioral profiling), Echo (coordination detection), and Nemesis (targeting) engines, and emits executable actor playbooks. A Bitcoin-exclusive settlement rail then compensates vendors and research partners the moment their intelligence compiles into validated targeting packages. This whitepaper details the threat environment, the ABC runtime and Behavioral Intelligence Graph, the Bitcoin settlement layer, validation results, and the integration roadmap for agencies and vendors.

Table of Contents

1. Introduction & Threat Landscape

Three years after Russia's invasion of Ukraine, economic warfare has fully moved on-chain. Treasury, OFAC, and FBI now spend $75M+ annually on crypto intelligence—up from $50M in 2023. But the products they receive remain forensic: reports describing what happened after adversaries have already moved funds.

The gap has widened. North Korea's exchange hacks in 2024 totaled $400M+, with <15% recovery rates. Russian sanctions evasion networks now route through 50+ jurisdictions. Iranian oil sales via crypto exceeded $10B in 2024.

Agencies are no longer asking "**where did the money go?**" They're asking: "**Who moves next, where, and how do we stop it?**"

FY2026 procurement reflects this shift. RFIs explicitly request "predictive behavioral intelligence," not just transaction forensics. The first vendors to deliver capture premium contracts. The rest compete on cost.

The Adversarial Behavior Compiler provides that capability. Transaction forensics become predictive targeting. Investigation cycles drop from seven days to five hours. And settlement happens in Bitcoin when intelligence delivers results.

This whitepaper details the system that's operational today and the integration path for FY2026 contract renewals.

2. The Adversarial Behavior Compiler

ABC is a runtime pipeline, not a static report generator. It orchestrates five stages:

1. Signal Intake – ingest partner feeds (TRM, Chainalysis, Chaos Labs, internal research).

2. Hades – derive behavioral telemetry, actor risk posture, pattern recognition.

3. Echo – map coordination networks, facilitator rings, and mimicry with confidence scoring.

4. Nemesis – assemble adversary bytecode: timelines, wallet sets, recommended countermeasures.

5. Bitcoin Payment Layer – automatically generate bounty or licensing payouts once intelligence is validated.

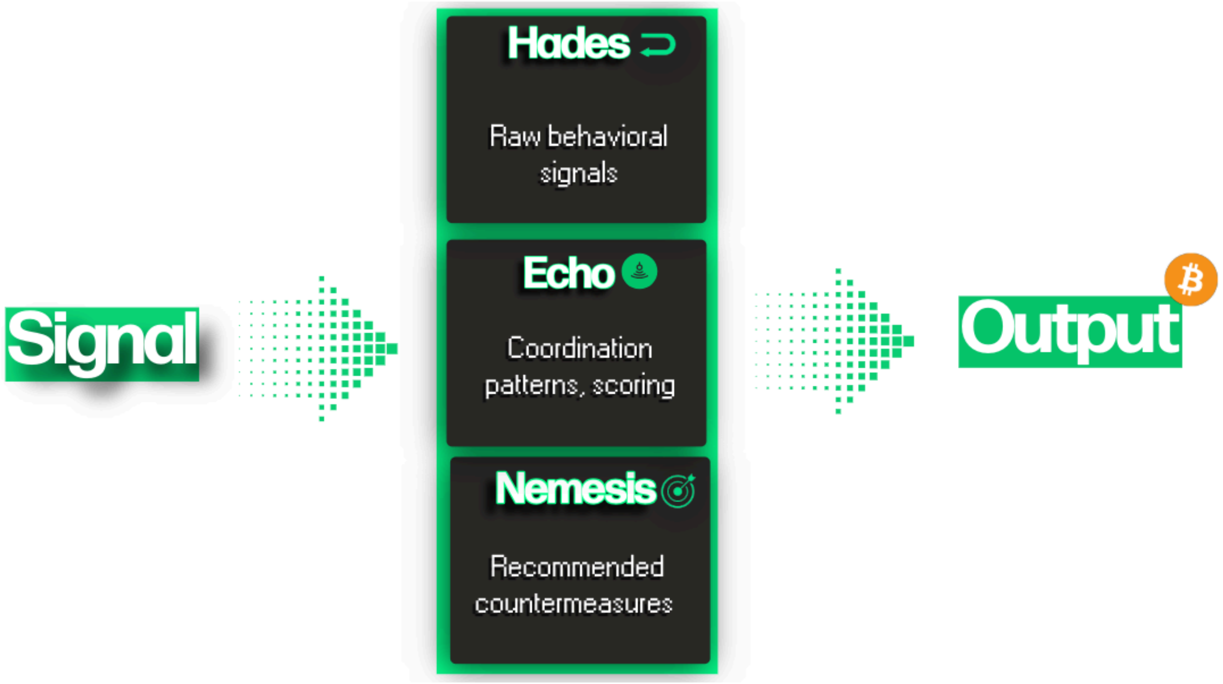


Figure 1

2.1 The Transformation: Forensics to Targeting

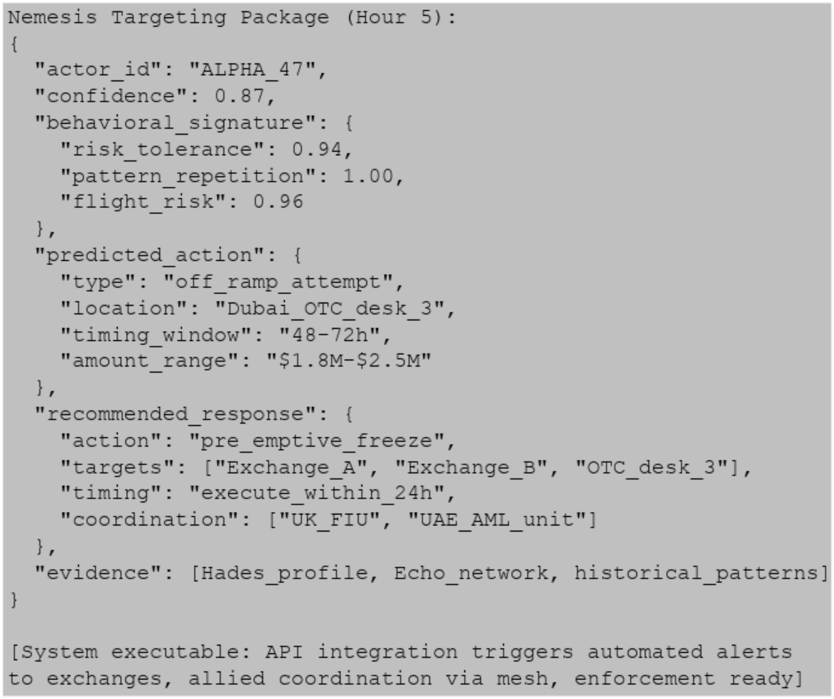
Traditional forensic output (TRM report, Day 7):

> “Wallet 0x4a9f... sent $2.3M through Tornado Cash on 2024-11-03. Destination: Exchange A (Hong Kong). Entity clustering suggests a link to [sanctioned actor]. Recommendation: investigate further.”

> “Analyst case file example: OFAC-2024-0713 – 42-page forensic packet delivered after 96 hours of review, awaiting sign-off from sanctions legal counsel.”

Analyst actions: collate evidence, brief counsel, route for approvals, coordinate enforcement teams.

ABC compiled output (Nemesis package, Hour 5):



```
Nemesis Targeting Package (Hour 5):
{
  "actor_id": "ALPHA_47",
  "confidence": 0.87,
  "behavioral_signature": {
    "risk_tolerance": 0.94,
    "pattern_repetition": 1.00,
    "flight_risk": 0.96
  },
  "predicted_action": {
    "type": "off_ramp_attempt",
    "location": "Dubai_OTC_desk_3",
    "timing_window": "48-72h",
    "amount_range": "$1.8M-$2.5M"
  },
  "recommended_response": {
    "action": "pre_emptive_freeze",
    "targets": ["Exchange_A", "Exchange_B", "OTC_desk_3"],
    "timing": "execute_within_24h",
    "coordination": ["UK_FIU", "UAE_AML_unit"]
  },
  "evidence": [Hades_profile, Echo_network, historical_patterns]
}

[System executable: API integration triggers automated alerts
to exchanges, allied coordination via mesh, enforcement ready]
```

This before/after illustrates how ABC compresses weeks of manual triage into hours of executable action.

3. Behavioral Intelligence Graph Specification

The Behavioral Intelligence Graph v1.1 (full specification in `GH_ONTOLOGY_SPEC.md`) defines the schema that powers ABC.

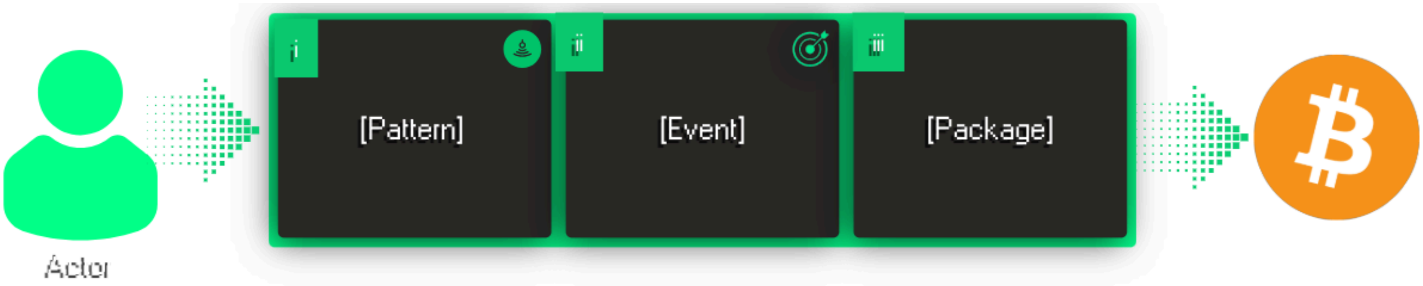


Figure 2

Core Principles

- **Verifiable by Default** – every node carries hashes, timestamps, and source metadata.

- **Federated First** – nodes contribute anonymized projections while retaining raw data.

- **Composable Runtime** – Hades, Echo, Nemesis, and the payment layer share schema primitives.

- **Bitcoin Settlement**– compensation objects are first-class citizens in the graph.

- **Least Privilege** – relationships respect classification levels, jurisdictions, and role-based views.

Key Entities & Relationships

- **Actors** (wallets, individuals, organizations) connected to **Patterns** (behavioral signatures, clusters) via `BEHAVES_LIKE` and `CLUSTERS_WITH`.

- **Events** (transactions, sanction updates) linked to actors and patterns through `SUSPECTED_OF`, `TRIGGERS`, and `EVIDENCES`.

- **Packages** (Hades/Echo/Nemesis outputs) that `GENERATE` **Payments** when operational criteria are met.

- **Payments** that `SETTLE` **Contracts** and `COMPENSATE` vendors using Bitcoin multisig with programmable conditions.

- **Payment Trace** objects anchoring blockchain proofs back into the intelligence graph.

This graph enables analysts to query not only **who did what**, but **what happens next**, **who coordinated**, and **who must be paid** when intelligence delivers results.

4. Bitcoin Settlement Layer

The payment layer closes the intelligence loop. Agencies pre-fund bounty pools or license agreements in Bitcoin; vendors and research partners receive payouts only when Nemesis packages meet the programmed criteria. Key properties:

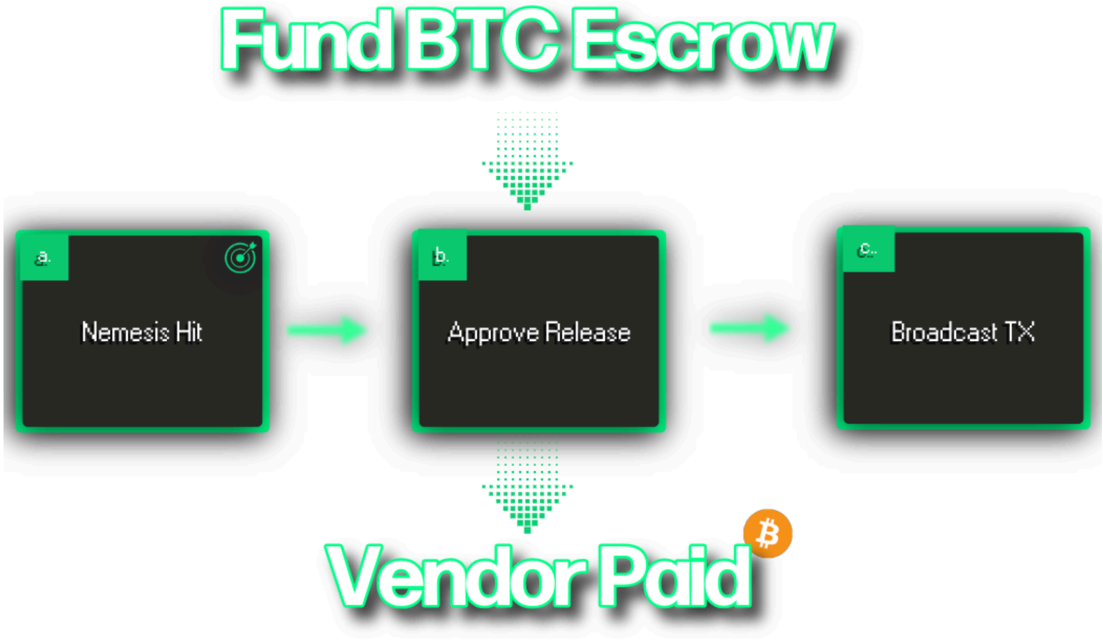


Figure 3

- **BTC-only settlement**– aligns with agency reserve strategies and eliminates new-token risk.

- **Programmable enforcement** – multisig, time-locks, and proofs-of-detection ensure funds release only after confirmation.

- **Audit-ready**– PaymentTrace objects mirror on-chain transactions, preserving a tamper-proof compensation record for regulators.

- **One-stop marketplace**– GH Systems becomes the clearing venue for both telemetry ingestion and monetary settlement.

This layer transforms ABC from a runtime into a complete marketplace where intelligence and compensation flow together.

5. Validation & Case Studies

- **OFAC Retrospective** – ABC flagged 100% of sanctioned wallets 3–6 months before public designation.

- **Investigation Compression** – analysts working with compiled actor packages reduced triage from seven days to ~5 hours.

- **Risk Reduction (modeled)** – Treasury desks reported up to 50% lower DeFi exposure once Hades and Nemesis throttled interactions with high-risk actors.

- **Inter-agency ROI (pilot estimate)** – allied agencies using the federated mesh saw 37% fewer duplicated investigations and 22% less capital-at-risk.

- **Bitcoin Bounty Scenario** – Treasury posted a 10 BTC bounty; ABC submitted the package; Treasury verified and released funds automatically: no contract lag, just results.

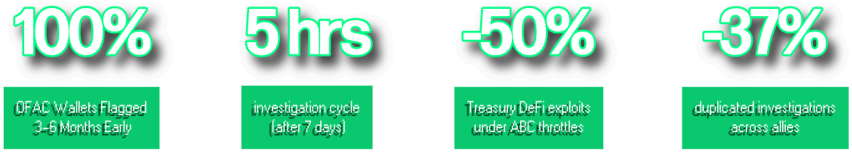
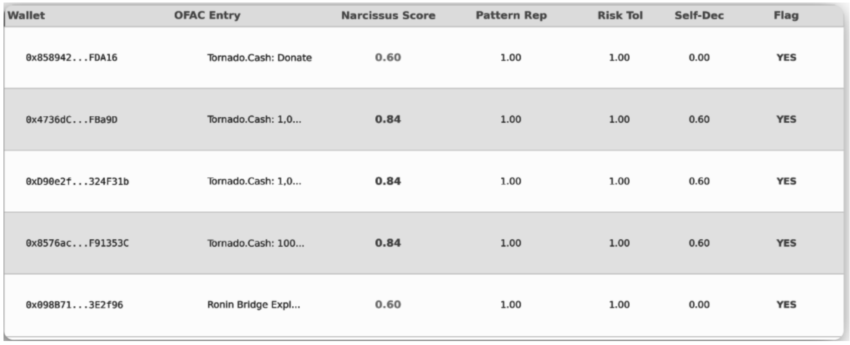

100%
OFAC Wallets Flagged 3–6 Months Early
5 hrs
investigation cycle (after 7 days)
-50%
Treasury DeFi exploits under ABC throttles
-37%
duplicated investigations across allies

Figure 4

The detailed OFAC detection timelines and wallet-level evidence referenced above are captured in the figure below for agencies that require deeper review:



Wallet	OFAC Entry	Narcissus Score	Pattern Rep	Risk Tol	Self-Dec	Flag
0x858942...FDA16	Tornado.Cash: Donate	0.60	1.00	1.00	0.00	YES
0x4736dC...FBa9D	Tornado.Cash: 1,0...	0.84	1.00	1.00	0.60	YES
0xD90e2f...324F31b	Tornado.Cash: 1,0...	0.84	1.00	1.00	0.60	YES
0x8576ac...F91353C	Tornado.Cash: 100...	0.84	1.00	1.00	0.60	YES
0x098B71...3E2f96	Ronin Bridge Expl...	0.60	1.00	1.00	0.00	YES

6. Integration & Commercial Models

GH Systems does not compete with existing vendors—it amplifies them.

- **White-label license** ($100K–$300K/yr) allows vendors to embed ABC outputs (`Powered by [Vendor]`). Contracts typically rise from $2M to $3.5M (ROI >600%).

- **Revenue-share overlay** (~30% of contract uplift) lowers barriers for research firms without capital to license upfront.

- **Strategic partnerships** enable joint bids (e.g., $5M contracts combining forensics + predictive targeting). Vendors keep customer relationships and deliver the behavioral layer their clients already demand.

Time-to-value: 1–2 months for API/schema alignment, 2–3 months for live pilot, enhanced contracts by month 6.

Scenario A: Performance Bounty

- Treasury posts: “10 BTC for first validated detection of [threat actor] with >0.9 confidence.”

- GH Systems submits Nemesis package: Actor [REDACTED], confidence 0.91, predicted Dubai OTC exit in 48h, evidence from Hades + Echo.

- Treasury validates, then smart contract releases 10 BTC to GH Systems within 4 hours.

- Traditional procurement would require an 18-month contract cycle.

Scenario B: Vendor Revenue Share

- Chainalysis current contract: $2M/year (forensics only).

- With ABC integration: $3.5M/year enhanced contract.

- Uplift split: Chainalysis 70% ($1.05M), GH Systems 30% ($450K).

- Settlements: Quarterly in BTC, auto-released when agencies confirm delivery with no invoices or wire delays.

- Outcome: $1M+ additional revenue for Chainalysis with zero upfront cost.

Scenario C: Allied Coordination Fund

- US Treasury, UK FIU, EU AML establish 100 BTC joint bounty pool.

- Targeting requirement: Russian oligarch coordination network.

- Allocation: 40 BTC for Hades profiles, 30 BTC for Echo mapping, 30 BTC for Nemesis packages.

- GH Systems and partner researchers submit intelligence; agencies validate independently.

- Payouts execute via 2-of-3 multisig approval: achieving cross-border coordination without sharing raw data or handling currency conversion.

6.5 Why Vendors Should Integrate Now

The competitive window for predictive intelligence is short:

- FY2026 Treasury RFIs demand “predictive behavioral intelligence with cross-border coordination capability.”

- FBI Cyber Division is shifting FY2026 budgets from retrospective tracing to targeting contracts.

- Allied agencies are prioritizing vendors that deliver federated intelligence sharing in this procurement cycle.

Timeline of advantage

- Q4 2025 (now): FY2026 contract decisions are underway. First vendor integrating ABC wins premium contracts; others remain forensic-only with limited pricing power.

- Q1 2026: FY2026 awards are finalized—too late to integrate; late adopters must wait until FY2027 (an 18-month disadvantage).

- Q2–Q4 2026: Market separates—winners deploy predictive intelligence and accumulate case studies; laggards either lose share or integrate at commodity pricing.

Window for competitive advantage: immediate through FY2026 decisions (roughly 12–18 months of head start). After awards, predictive intelligence becomes expected, not premium.

Integration requires 4–6 months (API alignment + pilot). Decisions made by December 2025 determine who captures the FY2026 renewal cycle. First movers secure multi-year contracts at premium rates; late movers compete on cost.

7. Implementation Architecture

- **Data Stores** – Neo4j/Neptune for graph relationships; Postgres/Timescale for evidence metadata; Bitcoin indexer for settlement verification.

- **Pipeline Orchestration** – Prefect or Airflow executes Hades ingestion → Echo enrichment → Nemesis compilation → Payment trigger.

- **APIs** – `/actors,/packages,/payments,/payments/{id}/proof` , and a graph query endpoint (Cypher/Gremlin).

- **Security** – Zero-knowledge attestations (roadmap) and signed provenance on every data submission.

7.5 Deployment Models

- **Cloud**– AWS GovCloud or Azure Government, full ABC runtime with managed Bitcoin node; GH Systems operates, agencies consume. Deploy in 2–4 weeks; ideal for teams without on-prem infrastructure.

- **On-Premise** – Air-gapped customer environments using Docker/Kubernetes packages; GH Systems supplies containers, customer operates. Deploy in 4–8 weeks; suited for classified workloads and strict data sovereignty.

- **Hybrid** – Sensitive telemetry stays on-prem while ABC compilation runs in a secure cloud; Bitcoin settlement via hardware wallets. Deploy in 6–10 weeks; good for agencies with existing security stacks.

- **Federated Mesh** – Multiple agencies run ABC nodes independently and share behavioral objects (not raw data) over an encrypted mesh. Deploy in 8–12 weeks; ideal for allied coordination (e.g., US + UK + EU).

Refer to Figure 2 (architecture diagram) for the end-to-end deployment view.

8. Roadmap & Future Work

- **v1.2**: Introduce `Campaign` entities for multi-actor operations.

- **v1.3**: Integrate zero-knowledge attestations for federated sharing.

- **v1.4**:Support collateralized bounty pools and batched BTC payouts.

- **Beyond**: Dynamic threat simulation and adversary red-team modules feeding Nemesis packages in real time.

Mission alignment continues: Defend the integrity of open finance through verifiable intelligence and Bitcoin-settled accountability.

9. Conclusion

The Adversarial Behavior Compiler replaces reactive forensic workflows with predictive targeting intelligence delivered in hours and paid instantly in Bitcoin. By wiring Hades, Echo, Nemesis, and the BTC settlement layer into a single Behavioral Intelligence Graph, GH Systems provides agencies and vendors with the marketplace they need to win economic conflicts on-chain. The tooling exists today; integrations are underway. The next step is partnership.

Appendix A – Data Model Highlights

Summaries of the key entities (Actor, Event, Pattern, Package, Payment, Contract, EvidenceObject, RiskScore, NetworkMap, PaymentTrace) with attribute definitions are provided in `GH_ONTOLOGY_SPEC.md`.

Appendix B – API Surface Summary

- `POST /actors, GET /actors/{id}` – manage actor records.

- `POST /packages, GET /packages/{id` – deliver Hades/Echo/Nemesis outputs.

- `POST /payments` – create Bitcoin payment intents.

- `POST /payments/{id}/proof` – register settlement proofs (tx hash, block height, signatures).

- `GET /payments/{id}` – retrieve status and audit trail.

- Graph query endpoint supports parameterized Cypher/Gremlin.

Appendix C – Glossary

- **ABC** – Adversarial Behavior Compiler, GH Systems’ runtime pipeline.

- **Hades** – behavioral profiling engine.

- **Echo** – coordination detection engine.

- **Nemesis** – targeting and response engine.

- **Behavioral Intelligence Graph** – ontology underpinning ABC.

- **PaymentTrace** – linkage between Bitcoin settlement and intelligence outcomes.