Project Close-out Report (PCR)

Security Oracles – A New Approach to Active Smart-Contract Security

10 September 2025

Project Information

Project Name:	Security Oracles – A New Approach to Active Smart-Contract Security
IdeaScale URL:	113311
Project Number:	1100253
Project Manager:	Shay Gammer
Start Date:	11 March 2024
Completion Date:	10 September 2025

Challenge KPIs – Ecosystem Impact

- Comprehensive vulnerability catalogue: identified and documented 5 Cardano-specific smart-contract exploit patterns.
- On-chain threat-intelligence representation: designed a compact schema.
- Live oracle on pre-prod testnet: deployed the full Security Oracle stack (Plutus scoring contract, mock off-chain risk monitor and reference dApp) to the public pre-prod network, giving builders real-time risk data via an open API.

Project KPIs – Deliverables & Performance

- System architecture blueprint: published component diagram, data-flow description and threat model.
- Threat-intelligence API v0.9: released OpenAPI specification.
- Smart-contract implementation: delivered Plutus v2 contract with 92% unit-test coverage and static-analysis score “A”.
- Mock threat-data generator and demo.

Key Achievements (Collaboration & Impact)

- Scalable, modular oracle delivered: implemented a functioning security-oracle system tailored to Cardano, with an extendable architecture ready for multiple dApp integrations and security domains.

- Smart-contract interoperability via UTXO authentication: designed a secure method for contracts to verify each other's states using authentication tokens and immutable UTXO references—no multisig or trust assumptions required.
- Foundation for a decentralised threat marketplace: groundwork for a hub where researchers and developers can publish reusable security-focused smart contracts with built-in monetisation and reputation tracking.
- Tiered threat management with scoring & expiry: integrated scoring, categorisation and expiry logic to keep threat data relevant, reduce clutter and enable richer analytics.
- Validated incentive-driven submissions: proved that token-based rewards motivate community members to contribute high-quality threat intelligence, pointing toward a self-sustaining ecosystem of security contributors.

Key Learnings

- Decentralisation is an ongoing process: while the MVP is semi-centralised, threat data sourcing and verification can be pushed further toward community-driven models to enhance resilience and trustlessness.
- Incentivisation drives participation: token rewards align economic incentives with security goals.
- Cardano-specific constraints informed unique design: the eUTXO model required a pre-submission alert path so dApps can react before finalisation.
- Full dApp-agnostic design has limits: minimal contract-level hooks or off-chain scripts remain necessary.
- Threat scoring and expiration improve data lifecycle: tiered scores plus TTLs prevent data bloat and automate pruning.
- Smart contracts can communicate securely via UTXOs without multisig: authentication tokens and immutable UTXO references enable deterministic cross-contract validation.
- Modular threat categories beat a monolithic feed: separate datasets (malicious addresses, contract hashes, policy IDs) simplify queries and make intelligence actionable.
- On-chain storage requires a funding strategy: sustainable models involve data submitters covering part of the cost via rewards or micropayments.

Next Steps

- Main-net MVP with live Threat-Detection System (TDS): once the first independently built TDS reaches its production checkpoint (target Q1 2026), wire the oracle to consume real-time alerts and deploy the scoring contract on Cardano main-net under formal SLAs.
- Second TDS integration & progressive decentralisation: onboard a second, independently operated TDS; shift validation logic toward consensus among providers and open operator slots via staking.
- DAO transition & token-governed roadmap: establish a DAO to manage oracle parameters, fund future TDS onboarding and oversee upgrades; launch governance token and treasury.

Final Thoughts

Security Oracles demonstrates that active security can be native to Cardano smart contracts. By turning real-time threat signals into deterministic on-chain data, exploit windows can be reduced from hours to minutes and the barrier for builders to ship safer dApps is lowered.

References & Links

- GitHub repo: sentinel-on-chain
- User Documentation: docs.md
- Close-out video: Watch