Assure DeFi®

THE VERIFICATION GOLD STANDARD

Security Assessment

SyntorAI

Date: 10/06/2025

Audit Status: PASS

Audit Edition: Advanced

ASSURE DEFI®

THE VERIFICATION GOLD STANDARD

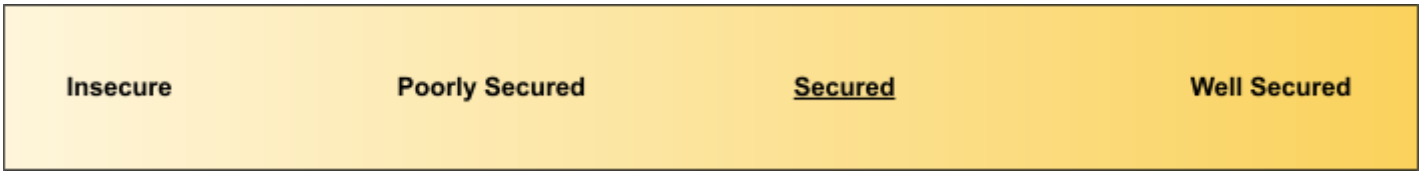
Risk Analysis

Vulnerability summary

Classification	Description
High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

Executive Summary

According to the Assure assessment, the Customer's smart contract is **Secured.**



Scope

Target Code And Revision

For this audit, we performed research, investigation, and review of the SyntorAI contracts followed by issue reporting, along with mitigation and remediation instructions outlined in this report.

Target Code And Revision

Project	Assure
Language	Solidity
Codebase	https://etherscan.io/address/0x21e133E07b6CB3FF846B5a32Fa9869a1E5040da1#code Ownership renounced TX: https://etherscan.io/tx/0x41e162fa04e74f4193419dee1e047beb32fea3829cd23976a8e8c5e156337d31
Audit Methodology	Static, Manual

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Category	Item
Code review & Functional Review	• Compiler warnings. • Race conditions and Reentrancy. Cross-function race conditions. • Possible delays in data delivery. • Oracle calls. • Front running. • Timestamp dependence. • Integer Overflow and Underflow. • DoS with Revert. • DoS with block gas limit. • Methods execution permissions. • Economy model. • Private user data leaks. • Malicious Event log. • Scoping and Declarations. • Uninitialized storage pointers. • Arithmetic accuracy. • Design Logic. • Cross-function race conditions. • Safe Zeppelin module. • Fallback function security. • Overpowered functions / Owner privileges

AUDIT OVERVIEW

HIGH

---

1. Reentrancy via external call [Mitigated ✅]

Issue: ETH transfers to project & operations wallets use unguarded call, enabling reentrant entry into contract.

Recommendation: Use a ReentrancyGuard or pull-over-push pattern; send ETH after updating all state and before external calls.

Fix: Ownership is renounced, all addresses are verified as safe. The risk now is LOW.

MEDIUM

---

1. Denial-of-Service on swap due to failing wallet call [Mitigated ✅]

Issue: If OperationsWallet or ProjectWallet is a contract whose fallback reverts, _exchangeTokensForEth reverts and blocks swaps.

Recommendation: Wrap external calls with try/catch or use send with a gas stipend and log failures without reverting; add emergency withdraw.

Fix: Ownership is renounced, all addresses are verified as safe. The risk now is LOW.

2. Signature replay & domain mismatch [Acknowledge ✅]

Issue: EIP-712 domain uses name “Trading Token” and omits a nonce deadline, allowing replay of the owner’s signature.

Recommendation: Align domain name with token ("Syntor AI"), include a deadline and per-call nonce in the signed data.

LOW

1. Missing to != address(0) check [N/A ✅]

Issue: Transfers to the zero address aren't explicitly prevented (though treated as burns), potentially unintended.

Recommendation: Add require(to != address(0), "ERC20: transfer to the zero address").

Fix: Ownership is renounced, all addresses are verified as safe.

2. Single swap per block limiter may be circumvented [Acknowledge ✅]

Issue: Tracking _swapCount only by block number allows exactly one swap, but could still be gas-heavy in tight loops.

Recommendation: Consider gas-cost checks or on-chain frequency capping, and expose manual swap abort mechanisms.

INFORMATIONAL

1. Owner centralization & lack of transparency [Fixed ✅]

Issue: Owner can change economic parameters (adjustTaxRates, setSwapThresholds, disableLimits) without on-chain governance or events.

Recommendation: Emit dedicated events for changes to fees, thresholds, and limits; consider timelocks or multisig for critical updates.

2. Gas inefficiencies & lack of immutables [Acknowledge ✅]

Issue: Wallet addresses and fee rates are regular state variables, incurring extra gas per access.

Recommendation: Mark constant values and wallet addresses as immutable or constant to save gas.

Technical Findings Summary

Findings

Vulnerability Level	Total	Mitigated	Not Apply	Acknowledged	Partially Fixed	Fixed
High	1	1				
Medium	2	1		1		
Low	2		1	1		
Informational	2			1		1

Assessment Results

Score Results

Review	Score
Global Score	**90/100**
Assure KYC	Not completed
Audit Score	90/100

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit PASS

Following our comprehensive security audit of the token contract for the SyntorAI project, we inform you that the project has met the necessary security standards.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocating for the Project, and users relying on this report should not consider this as having any merit for financial adSyntorAI in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment adSyntorAI, nor should it be used to signal that any person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment serSyntorAIs provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any serSyntorAIs, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The serSyntorAIs may access, and depend upon, multiple layers of third parties.