ELITE SHIELD

Product Use Case Overview

Powered by Elite Oracle · Advanced Onchain Risk Detection

Figure 1 — Elite Shield Landing Interface

Prepared by	Document Type	Version	Date
Elite Oracle Team	**Product Overview**	**1.0**	**February 19, 2026**

1. Executive Summary

Elite Shield is the flagship onchain risk intelligence platform developed by Elite Oracle — a next-generation blockchain security company dedicated to protecting retail and institutional participants from fraudulent, manipulative, and high-risk digital assets. Built atop a powerful AI-driven analysis engine and integrated directly with GoPlus Security's industry-leading smart contract data infrastructure, Elite Shield delivers institutional-grade security assessments in a matter of seconds, making sophisticated due diligence accessible to any market participant.

The platform addresses one of the most persistent pain points in the decentralised finance (DeFi) ecosystem: the ability to quickly and reliably assess whether a token or smart contract poses a genuine risk before capital is deployed. Elite Shield solves this by combining real-time on-chain data, multi-layered behavioural honeypot detection, and a proprietary three-layer security scoring model — all surfaced through a clean, intuitive interface requiring no technical expertise from the end user.

Core Value Proposition

- **Instant Analysis** — Security results delivered in seconds, not hours.
- **Multi-Signal Intelligence** — Combines honeypot detection, tax analysis, holder distribution, and LP lock status in a single view.
- **AI-Powered Audit Engine** — Smart Contract Audit with AI scoring produces a trusted, reproducible security score.
- **Exportable Reports** — Full audit PDFs generated on-demand for compliance, sharing, and record-keeping.
- **Multi-Chain Support** — Covers Ethereum, and all major EVM-compatible and Solana-based chains.

2. How Elite Shield Works

The Elite Shield workflow is designed for maximum simplicity without sacrificing analytical depth. The entire end-to-end process — from contract submission to full audit report — is completed within a single browser session, requiring no wallet connection, registration, or technical background.

STEP 1	**Paste the Contract Address** The user navigates to the Elite Shield interface and pastes any EVM-compatible or Solana contract address into the search bar. The platform supports all major chains automatically — no manual network selection required.
STEP 2	**Click ANALYZE** Upon clicking the ANALYZE button, Elite Shield instantly retrieves on-chain data from DexScreener and GoPlus Security APIs. Within seconds, the platform displays a comprehensive Token Summary panel covering price, liquidity, volume, market cap, token age, buy/sell ratio, and multi-timeframe price analysis.
STEP 3	**Review the Security Dashboard** The user is presented with a full security dashboard including: a composite Security Score, a Rug Alert banner where applicable, Honeypot Detection Results with probabilistic scoring, a Liquidity Breakdown, an AI Analysis summary, and a Detailed Report covering all critical on-chain metrics.
STEP 4	**Run the Smart Security Audit** By pressing the SMART SECURITY AUDIT button, the AI Audit Engine performs a 21-point smart contract audit powered by GoPlus Security. Results are displayed in real time — covering compiler integrity, reentrancy, integer overflow, tax model, holder permissions, and 17 additional checks — all categorised by severity level.
STEP 5	**Export the Audit PDF** The completed audit report can be exported as a professionally formatted PDF in a single click. The exported document includes the full audit checklist, security flags, holder analysis, LP lock status, three-layer score breakdown, and a signed conclusion — suitable for sharing with investment teams, community members, or compliance stakeholders.

3. Interface Walkthrough

3.1 Landing Screen

The Elite Shield landing page presents users with a minimal, distraction-free interface. A single search field labelled with placeholder text accepts any contract address across all supported chains. Recent scans are surfaced below the search bar for rapid re-access. The clean design ensures that even first-time users can immediately begin an analysis without guidance.

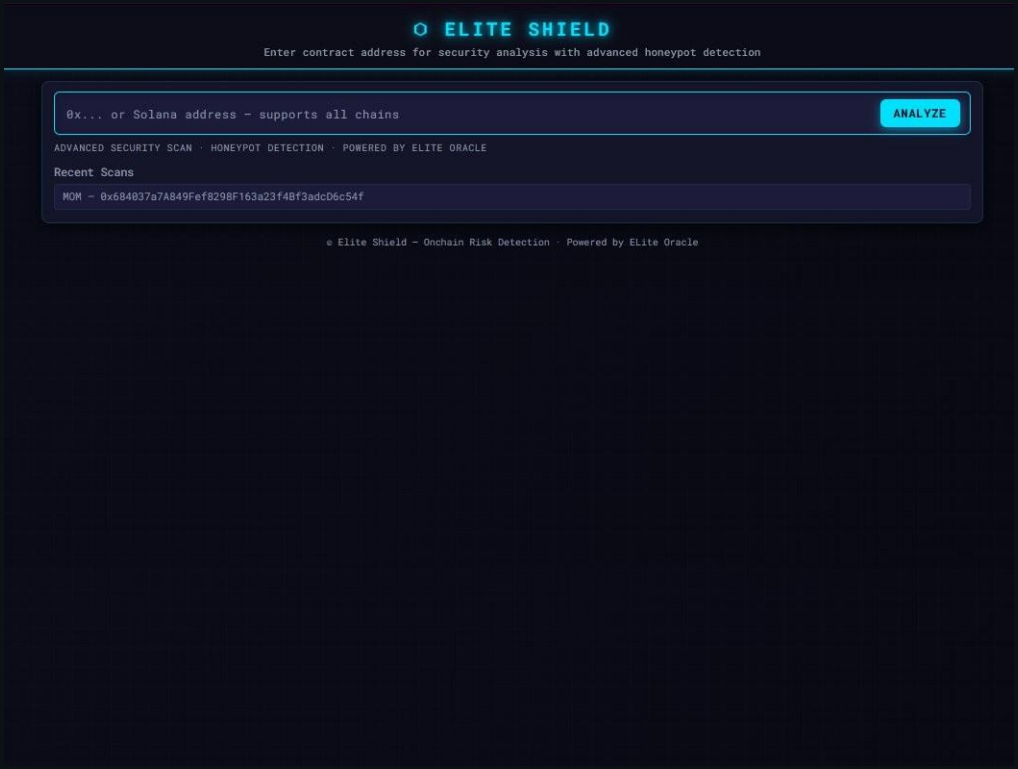


Figure 2 — Elite Shield landing screen. Users simply paste a contract address and click ANALYZE.

3.2 Token Summary & Market Intelligence

After analysis, the left panel displays a Token Summary containing every market metric a trader or researcher needs for initial evaluation: real-time price, fully diluted valuation (FDV), 24-hour volume, liquidity depth, transaction count broken down by buys and sells, token age, and chain/pair information. A colour-coded Rug Alert banner is prominently displayed for tokens flagged as high risk. The right panel shows DEX Pair Details including live price changes across 5-minute, 1-hour, 6-hour, and 24-hour windows.

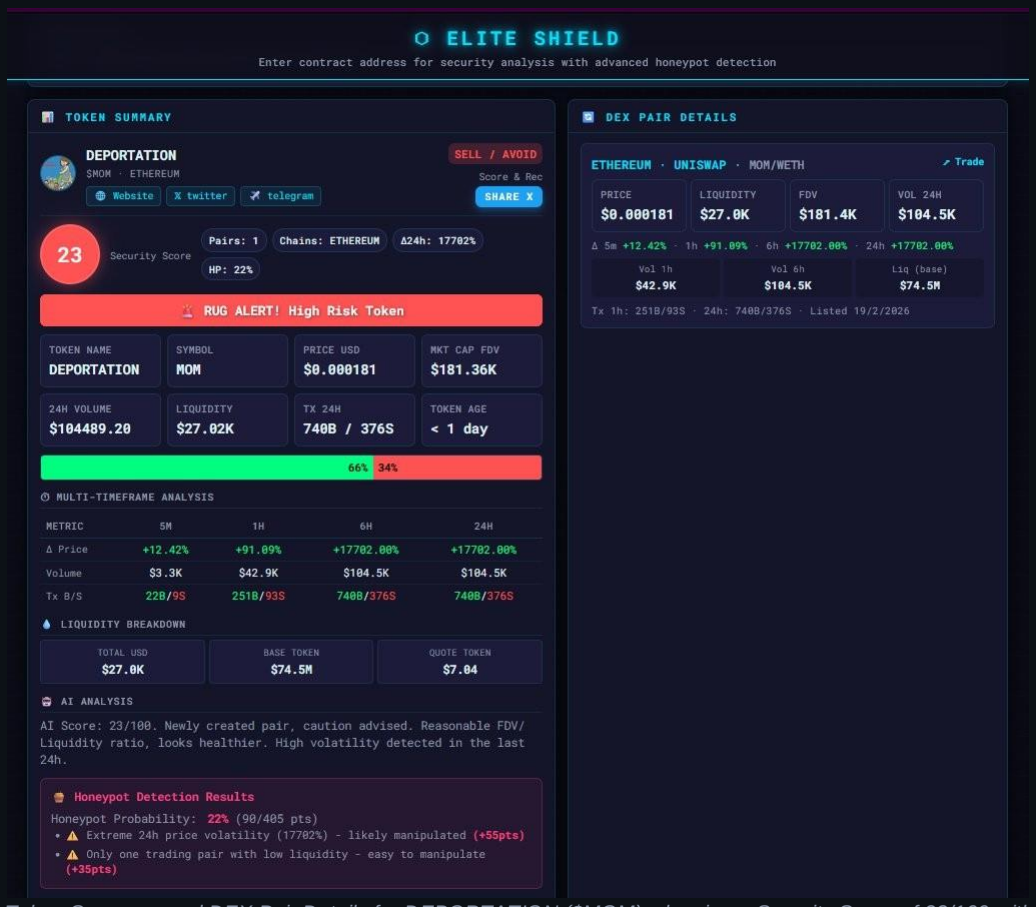


Figure 3 — Token Summary and DEX Pair Details for DEPORTATION ($MOM), showing a Security Score of 23/100 with Rug Alert.

3.3 AI Analysis & Honeypot Detection

Below the market data, Elite Shield surfaces an AI Analysis score and a Honeypot Detection Results section. The honeypot probability is expressed as a percentage derived from a points-based system (e.g., 90/405 pts), with individual risk factors listed alongside their point contributions. This transparent scoring approach allows users to understand precisely why a token has been flagged, rather than relying on opaque black-box verdicts. A Detailed Report section itemises every analysed dimension with pass/warn/fail indicators.

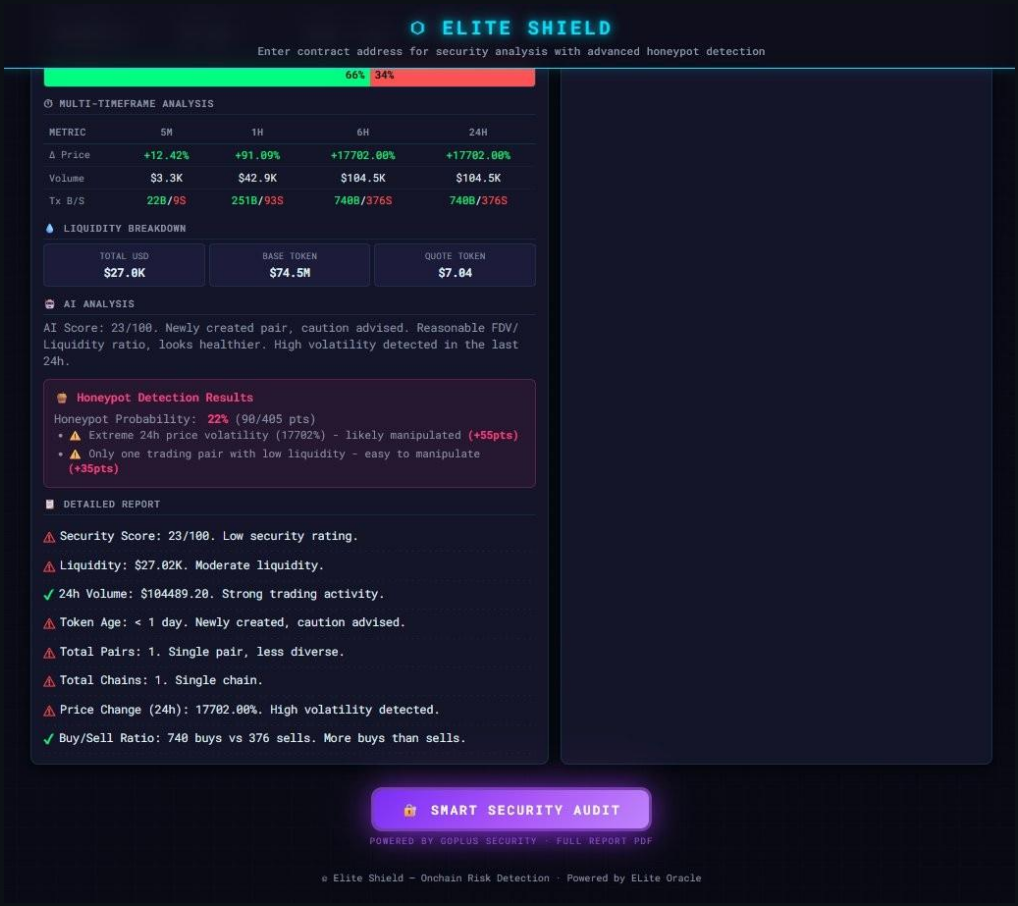


Figure 4 — AI Analysis, Honeypot Detection Results, and Detailed Report panel.

4. Smart Security Audit — AI-Powered Smart Contract Analysis

The Smart Security Audit is Elite Shield's most powerful feature. Triggered by a single button press, the AI Audit Engine performs a comprehensive 21-point security evaluation of the smart contract in real time. Unlike traditional manual audits that may take days or weeks, Elite Shield delivers a full audit result within seconds — making it the fastest credible security assessment available in the DeFi space.

4.1 Security Metrics Dashboard

The audit opens with a Security Metrics dashboard providing at-a-glance answers to the most critical binary questions: Is the contract open source? Is it a honeypot? What are the buy and sell tax rates? Can the token supply be minted? Is there a proxy or hidden owner? Is transfer functionality pausable? These metrics are sourced directly from GoPlus Security and displayed with clear YES/NO indicators, eliminating ambiguity.

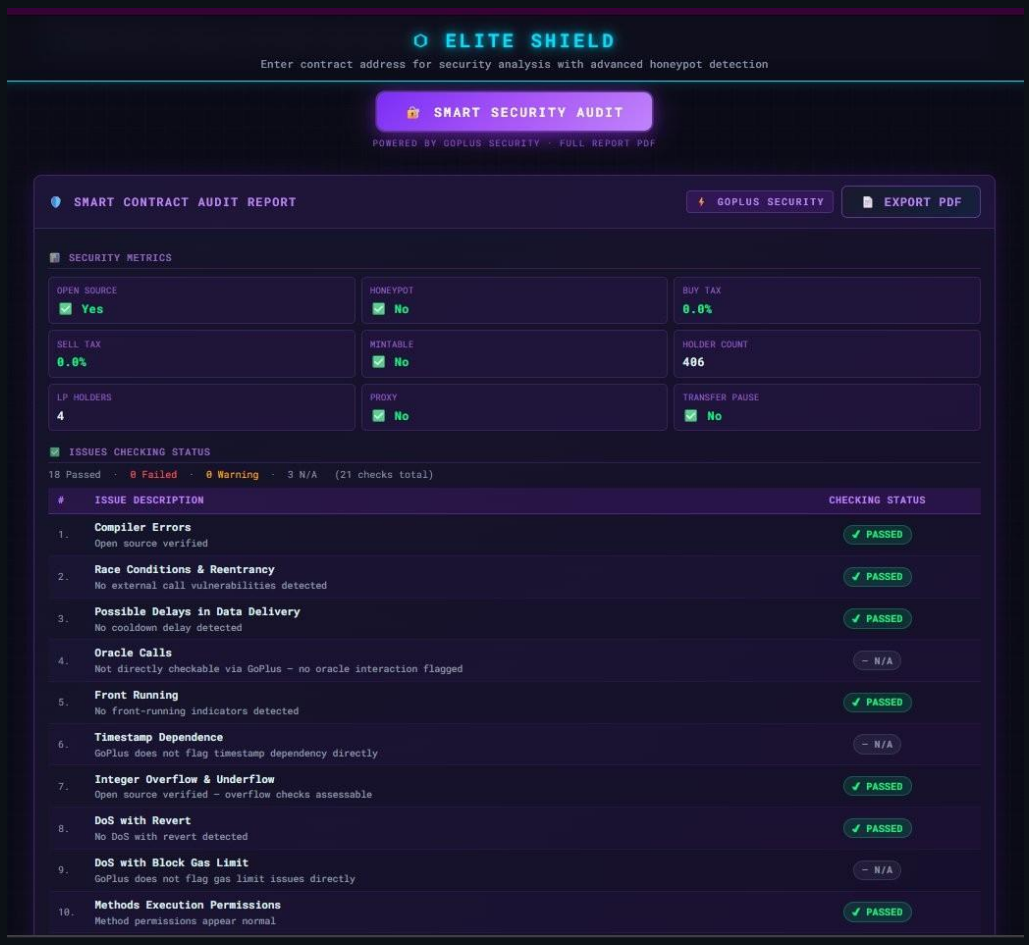


Figure 5 — Smart Contract Audit Report: Security Metrics and 21-point Issues Checking Status.

4.2 21-Point Issues Checklist

The core of the audit is a structured 21-point checklist covering every major smart contract vulnerability category recognised by the blockchain security industry. Each check is marked as Passed, N/A, or Failed, with a plain-English explanation of the methodology used. The checklist encompasses compiler integrity, race conditions and reentrancy, data delivery delays, oracle interactions, front-running exposure, timestamp dependence, integer arithmetic accuracy, denial-of-service vectors, execution permissions, economic model integrity, exchange rate logic, data leakage, event logging, scoping declarations, storage pointers, design logic, cross-function race conditions, OpenZeppelin implementation safety, and fallback function security.

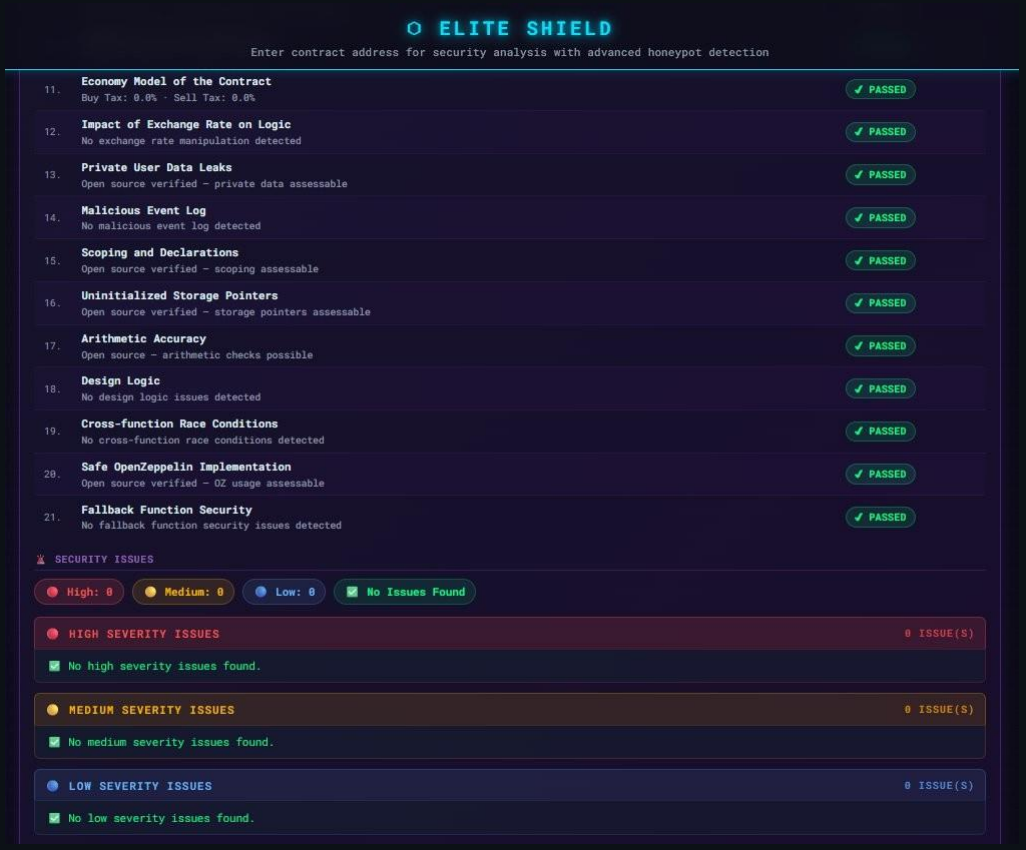


Figure 6 — Audit checklist items 11–21 with severity summary: 0 High, 0 Medium, 0 Low issues.

4.3 Contract Security Flags & Holder Analysis

A dedicated Contract Security Flags panel presents 14 binary security attributes in a structured grid, including honeypot status, open source verification, proxy contract detection, mintability, ownership takeback risk, balance modification capability, hidden owner detection, self-destruct function presence, external call exposure, buy/sell tax rates, trading cooldown, transfer pausability, blacklist function presence, anti-whale mechanisms, and slippage modifiability. Below this, a Top Holders table lists the largest token holders by address and percentage, enabling concentration risk assessment. Crucially, LP Holder data is also provided — showing whether liquidity is locked and through which protocol.

Figure 7 — Contract Security Flags panel and Top 10 Holder distribution with LP lock status.

4.4 Security Score & Three-Layer Scoring System

Elite Oracle's proprietary three-layer scoring model produces a final Audit Security Score out of 100. The architecture is designed to prevent gaming and ensure that fatal flags are never diluted by positive signals in other categories:

LAYER 1 — HARD GATE	Checks for absolute disqualifying conditions (honeypot detected, hidden owner, sell-all restriction, balance manipulation, selfdestruct). If any fatal flag is present, the score is hard-capped regardless of all other results.
LAYER 2 — CORE SECURITY (85% weight)	Four weighted sub-categories: Ownership & Control (30%), Trading Safety (25%), Holder Distribution (20%), and Honeypot Risk (10%). Each is graded A–F and contributes proportionally to the raw score.
LAYER 3 — CONTEXT MODIFIER	Applies positive and negative adjustments based on contextual signals: open source verification (+3%), LP lock (+3%), ownership renounced (+2%), token age under 3 days (-4%), single pair with low liquidity (-3%), extreme 24h price volatility (-2%). Net adjustment is added to the Layer 2 raw score to produce the final result.

Figure 8 — Final Audit Score (68/100), LP Holder lock confirmation, and three-layer score breakdown.

5. One-Click Audit Report Export

Every completed Smart Security Audit can be exported as a professionally formatted PDF report directly from the Elite Shield interface. The export feature — accessible via the EXPORT PDF button within the audit panel — generates a document that is suitable for distribution to investment teams, project communities, compliance officers, and exchange listing committees.

The exported PDF includes:

- Full project identification: contract address, token name, symbol, blockchain, and audit date.
- Complete 21-point Issues Checking Status table with pass/N/A classifications.
- Security Issues summary — categorised by High, Medium, and Low severity.
- Contract Technical Analysis covering all binary security flags.
- Top 10 Holder distribution table with percentage holdings and address tags.
- Top LP Holders table with lock status and protocol identification.
- Three-Layer Score Breakdown with sub-category grades and context modifiers.
- Final Audit Security Score and remediation status.
- Conclusion statement with Elite Oracle disclaimer and methodology reference.

The PDF is branded with Elite Oracle and Elite Shield identity and carries a timestamp, contract address, and score on the cover page — creating an immutable record of the security assessment at the time of analysis. This document can be referenced in governance proposals, community disclosures, or investment memoranda.

6. Target Use Cases & Audience

■ Retail Traders & Investors
Verify any new token before purchasing. Elite Shield provides an instant, jargon-free risk assessment that helps retail users avoid honeypots, rug pulls, and manipulated launches — without requiring any technical knowledge.

■ DeFi Research Analysts
Accelerate due diligence workflows. Analysts can screen dozens of contracts in the time it would take to manually review one, using Elite Shield as a first-pass filter before deeper fundamental analysis.

■ Project Teams & Token Developers
Demonstrate contract safety and transparency to prospective investors and community members. Exporting a clean audit PDF from Elite Shield provides an accessible, third-party-sourced security credential that builds confidence.

■ Crypto Influencers & KOLs
Conduct on-the-spot live contract analysis during streams, calls, or community sessions. Elite Shield's instant results make it ideal for real-time transparency demonstrations.

■ Launchpads & IDO Platforms
Screen projects submitting for listing or launch support. Integrate Elite Shield analysis into standard onboarding due diligence to protect the platform's reputation and user base.

■ Exchanges & Market Makers
Add an automated smart contract safety check into token listing evaluation processes, reducing the risk of listing high-risk or fraudulent assets.

7. Technology & Data Infrastructure

Elite Shield is built on a robust, multi-source data architecture that aggregates signals from the most trusted infrastructure providers in the blockchain security ecosystem:

GoPlus Security	Industry-standard smart contract security data provider. Supplies all binary security flags, tax data, holder information, and LP lock status used in both the token summary and the smart contract audit.
DexScreener	Real-time DEX market data aggregator providing live price feeds, volume metrics, liquidity depth, and transaction-level buy/sell data across all supported chains and trading pairs.
Elite Oracle AI Engine	Proprietary scoring and analysis layer that synthesises raw data into the three-layer security score, honeypot probability model, and natural-language AI analysis summary displayed in the platform.
Elite Shield	Web and mobile-accessible interface delivering results in a real-time, responsive dashboard with instant PDF export capability — requiring no wallet connection or user account.

8. Disclaimer

This document is provided for informational and product demonstration purposes only and does not constitute investment advice. Elite Oracle and its affiliates make no warranty or representation regarding the accuracy, completeness, or fitness for purpose of any security analysis produced by Elite Shield. Smart contract audit results reflect on-chain data available at the time of analysis and do not guarantee the future safety or performance of any digital asset.

Users are strongly advised to conduct their own independent due diligence before making any investment or transactional decisions. Past audit scores do not guarantee future security. Elite Shield analysis is not a substitute for a full manual code review by qualified smart contract security engineers.

SMART CONTRACTS
SECURITY AUDIT REPORT

DEPORTATION ($MOM)

0x684037a7A849Fef8298F163a23f4Bf3adcD6...

Powered by GoPlus Security · Elite Oracle · Elite Shield

February 19, 2026

Audit Details

Audited Project	DEPORTATION ($MOM)
Contract Address	0x684037a7A849Fef8298F163a23f4Bf3adcD6c54f
Client	DEPORTATION Team
Blockchain	ETHEREUM
Audit Date	February 19, 2026
Token Price (USD)	$0.000181
Market Cap / FDV	$181.36K
24h Volume	$104489.20
Liquidity	$27.02K
Token Age	< 1 day

Disclaimer

This is a limited report based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents.

Elite Oracle and its affiliates owe no duty of care towards you or any other person, nor does Elite Oracle make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind.

The analysis of the security is purely based on the smart contract data retrieved from GoPlus Security API and on-chain DEX data. No applications or operations were reviewed for security. No product code beyond the smart contract has been reviewed.

You should conduct your own independent investigation and due diligence before making any investment decisions. Past security audit results do not guarantee future safety.

Background

Elite Oracle was commissioned to perform a smart contract security audit:

```
0x684037a7A849Fef8298F163a23f4Bf3adcD6c54f
```

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended and expected.
- Identify potential security vulnerabilities within the smart contract code.
- Verify compliance with standard token security best practices.
- Assess honeypot risk, tax manipulation, and owner privilege concentration.
- Provide actionable findings categorized by severity level.

The information in this report should be used to understand the risk exposure of the smart contract. Security data was retrieved via GoPlus Security API and DexScreener.

Issues Checking Status

#	Issue Description	Checking Status
1.	**Compiler Errors** Open source verified	Passed
2.	**Race Conditions & Reentrancy** No external call vulnerabilities detected	Passed
3.	**Possible Delays in Data Delivery** No cooldown delay detected	Passed
4.	**Oracle Calls** Not directly checkable via GoPlus — no oracle interaction flagged	N/A
5.	**Front Running** No front-running indicators detected	Passed
6.	**Timestamp Dependence** GoPlus does not flag timestamp dependency directly	N/A
7.	**Integer Overflow & Underflow** Open source verified — overflow checks assessable	Passed
8.	**DoS with Revert** No DoS with revert detected	Passed
9.	**DoS with Block Gas Limit** GoPlus does not flag gas limit issues directly	N/A
10.	**Methods Execution Permissions** Method permissions appear normal	Passed
11.	**Economy Model of the Contract** Buy Tax: 0.0% · Sell Tax: 0.0%	Passed
12.	**Impact of Exchange Rate on Logic** No exchange rate manipulation detected	Passed
13.	**Private User Data Leaks** Open source verified — private data assessable	Passed
14.	**Malicious Event Log** No malicious event log detected	Passed
15.	**Scoping and Declarations** Open source verified — scoping assessable	Passed
16.	**Uninitialized Storage Pointers** Open source verified — storage pointers assessable	Passed

#	Issue Description	Checking Status
17.	**Arithmetic Accuracy** Open source — arithmetic checks possible	Passed
18.	**Design Logic** No design logic issues detected	Passed
19.	**Cross-function Race Conditions** No cross-function race conditions detected	Passed
20.	**Safe OpenZeppelin Implementation** Open source verified — OZ usage assessable	Passed
21.	**Fallback Function Security** No fallback function security issues detected	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

Contract Technical Analysis

OPEN SOURCE **Verified**	HONEYPOT **No**	BUY TAX **0.0%**
SELL TAX **0.0%**	MINTABLE **No**	PROXY **No**
TRANSFER PAUSE **No**	HOLDER COUNT **406**	LP HOLDERS **4**
HIDDEN OWNER **No**	BLACKLIST **No**	ANTI-WHALE **Active**

Contract Security Flags — Top Holders

Top 10 Holdings	Top 3 Holdings	Total Holders	Locked Found
17.3%	11.4%	10	No

#	Address / Label	Tag	% Holdings
1	UniswapV2	CONTRACT	Ø=ÜÄ 5%
2	0x22e4ba…74e28f		0.94%
3	0xe253ee…9cfc3e		0.90%
4	0xb0ea58…6b5aa5		0.90%
5	0x47f6fb…0dd16d		0.87%
6	0x44ec82…cc84aa		0.87%
7	0xdae4a0…69d642		0.85%
8	0x44efed…61db2d		0.83%
9	0x647648…fb09c2		0.82%
10	0xc8b48e…da74fa		0.81%

Top LP Holders

#	Address / Label		% LP
1	PinkLock02	Ø=Ý	99.81%
2	0xf38521…995f85		0.19%
3	0x23d5f7…edb500		0.00%
4	Null Address	Ø=Ý	0.00%

Security Score Breakdown

3-Layer Ideal Formula · No double counting · Hard Gate override

LAYER 1 · HARD GATE — No fatal flags detected. No score cap applied.

LAYER 2 · CORE SECURITY (weighted 85% of raw score)

Category	Data Source	Wt%	Score
A. Ownership & Control	Contract Security Flags / GoPlus ownership flags	100	A
B. Trading Safety	GoPlus Trading Flags + Tax Model (buy/sell tax)	100	A
C. Holder Distribution	Address / Tag table + LP Holders table	90	A
D. Honeypot Risk	Honeypot Detection Results (behavioral analysis)	79	B

LAYER 3 · CONTEXT MODIFIER (Token Summary + on-chain signals)

Signal	Applied	Pts
Open Source Verified	YES	+3%
Liquidity Provider Locked	YES	+3%
Ownership Renounced	YES	+2%
Token Age > 90 days	NO	—
Multi-chain presence	NO	—
Token Age < 3 days (very new)	YES	-4%
Single pair + low liq (<$50K)	YES	-3%
HP probability > 30%	NO	—
Price volatility > 200% (24h)	YES	-2%

Net Context: -1% !' -1 pts

Raw 69 + Context(-1) = 68 !' cap@100 = Final: 68

Remediation Status: Mitigated

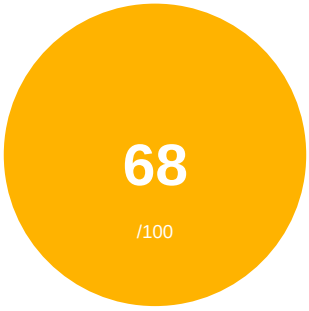
Mitigation evidence detected on-chain:

[OK] Source Verified **[OK] Owner Renounced** **[OK] LP Locked**

Hard Gate Reference — Fatal Flag Score Caps

CRITICAL	Honeypot Detected	MAX 10/100
CRITICAL	Cannot Sell All Tokens	MAX 20/100
CRITICAL	Hidden Owner	MAX 30/100
CRITICAL	Owner Can Modify Balances	MAX 30/100
CRITICAL	Selfdestruct Function	MAX 35/100
MAJOR	Ownership Reclaim Risk	MAX 40/100
MAJOR	Buy Function Disabled	MAX 40/100
CRITICAL	Buy or Sell Tax > 49%	MAX 25/100

Conclusion



AUDIT SECURITY SCORE

Smart contract audit completed via GoPlus Security. No high severity issues found. Always conduct your own due diligence before investing.

Smart contracts do not contain high severity issues!

Elite Oracle Note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the owner.