SCE

SAGITTA CONTINUITY ENGINE

CONFIDENTIAL

PUBLIC-SURFACE DEFENSE REVIEW REPORT

SAMPLE — STRUCTURE DEMONSTRATION

Demo report using Sagitta Protocol testnet deployment. Not a verified client result.

Sagitta Protocol

Prepared by Sagitta Continuity Engine (SCE) · May 20, 2026

RISK POSTURE — HIGH RISK

Shared owner concentration across 4 assets requires verification.

REVIEW ID **DR-2a10ffcdf2**	STATUS **Draft**
DATE ISSUED **May 20, 2026**	ENVIRONMENT **TESTNET**
ASSETS MAPPED **5**	OPEN FINDINGS **6**

Table of Contents

Sagitta Protocol · Public-Surface Defense Review · May 20, 2026

This report covers **6 open findings**, **4 relevant threat families**, and **29 evidence and control checks** across **5 mapped assets**.

01 EXECUTIVE SUMMARY

This report reflects a public-surface review of **Sagitta Protocol** conducted by Sagitta Continuity Engine (SCE). The analysis covers mapped public assets, authority risk findings derived from the Admin Surface Scanner, relevant global threat families, and recommended evidence and control checks. SCE does not control this project, hold keys, or execute on-chain transactions.

Primary Finding: Shared owner concentration across Treasury (Sagitta Protocol), Vault (Sagitta Protocol), Escrow (Sagitta Protocol), Reserve (Sagitta Protocol)

RISK POSTURE — HIGH RISK

2 high-risk authority surfaces require verification. These are unverified authority surfaces — not confirmed exploitable vulnerabilities.

ASSETS MAPPED	OPEN FINDINGS	CRITICAL / HIGH
5	6	0 / 2

THREAT FAMILIES	CONTROLS	CONTROLS VERIFIED	COVERAGE
4	29	0 / 29	0%

AUTHORITY PATHS RESOLVED	AWAITING EVIDENCE	EVIDENCE CHECKS VERIFIED
4 / 5	1 / 5	0 / 29

SCAN STATUS

Last scan:	May 20, 2026
Chains scanned:	Moonbase Alpha
Assets scanned:	5 / 5
Detector attempts:	Ownable, EIP-1967, Safe, Timelock, AccessControl
Scan status:	Complete
RPC config:	Scanned chain(s): [1287]

02 REVIEW SCOPE

This is a zero-custody public-surface review. SCE analyzes only publicly available metadata: contract addresses, deployment chains, admin surface indicators, and documented protocol configurations. No private keys, signing credentials, mnemonics, or seed phrases are requested or stored at any point.

Public-surface describes the data reviewed; Confidential describes distribution of this report.

> **NOT AN AUDIT**
> This Defense Review is not a full smart contract audit, formal verification report, penetration test, or economic exploit review. It is a zero-custody authority-surface and continuity-readiness review based on public metadata and submitted evidence.

Website: https://protocol.sagitta.systems/; Protocol Address Matrix import — moonbase / testnet

MAPPED CONTRACTS / PROXIES

CONTRACT **Vault (Sagitta Protocol)**
`0x30d987D24608E6D8A9A573c8B1290e2a0791356A`
moonbase / testnet
Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500 (resolved via Ownable.owner) - Role: vault

CONTRACT **Escrow (Sagitta Protocol)**
`0x6908b357995cFeD1008616E65Dbe428Cbd9dFA51`
moonbase / testnet
Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500 (resolved via Ownable.owner) - Role: escrow

OTHER MAPPED ASSETS

TREASURY **Treasury (Sagitta Protocol)**
`0xa4F62F8E07c85668678FDd48C2Fd982343b13687`
moonbase / testnet
Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500 (resolved via Ownable.owner) - Role: treasury

TREASURY **Reserve (Sagitta Protocol)**
`0xaf0E91C2fB084A50e2e8F207EE11468EA982a820`
moonbase / testnet
Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500 (resolved via Ownable.owner) - Role: reserve

ORACLE **Goldoracle (Sagitta Protocol)**
`0x8A2F00Ba2E27b34d834Be83041D09632B0627056`
moonbase / testnet
Admin/Owner: Unresolved - Role: goldoracle

03 SEVERITY METHODOLOGY

Severity in this report reflects potential impact to protocol continuity, fund safety, and operational control — not confirmed exploitation. Findings represent authority surfaces requiring verification; severity may be revised once evidence is provided and verified.

CRITICAL Direct fund movement, settlement, or custody authority with no timelock or multisig protection. Immediate risk to assets or protocol operation.

HIGH Significant authority surface — upgrade control, oracle authority, or admin role concentration — where verification evidence is absent or incomplete. Blast radius is large; unverified control paths.

MEDIUM Authority surface with limited or indirect fund impact, or where partial mitigations exist. Verification is recommended to confirm continuity posture.

LOW Informational or structural finding. Low direct risk but relevant to continuity planning, role documentation, and future audits.

> High-risk authority surfaces in this report represent unverified control paths — not confirmed vulnerabilities. Many findings reflect missing evidence rather than confirmed risk. Likelihood and verification confidence are factored into severity.

04 AUTHORITY RISK FINDINGS

HIGH-RISK AUTHORITY SURFACES REQUIRING VERIFICATION (2)

HIGH ROLE CONCENTRATION

Shared owner concentration across 4 assets — Treasury (Sagitta Protocol), Vault (Sagitta Protocol), Escrow (Sagitta Protocol), Reserve (Sagitta Protocol)

SCE resolved the same owner address (0xc643a9e5780420a939ced80e537f19bbe2d7c500) on 4 project assets: Treasury (Sagitta Protocol), Vault (Sagitta Protocol), Escrow (Sagitta Protocol), Reserve (Sagitta Protocol). This shared owner path is the primary continuity finding. Verify whether the owner is an EOA, multisig, timelock, or governed contract. Controls are not verified until the owner operating model, signer policy, multisig or timelock configuration, and emergency procedures are provided.

CURRENT EVIDENCE STATUS

· Source: EVM detector scan - Ownable.owner() cross-asset aggregation
Assets affected: Treasury (Sagitta Protocol), Vault (Sagitta Protocol), Escrow (Sagitta Protocol), Reserve (Sagitta Protocol)
Shared owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500
Owner Evidence Confidence: verified
Control Verification: incomplete
Evidence Source: EVM detector scan - Ownable.owner() cross-asset aggregation
Detection Method: eth_call owner()
Detection Result: Same owner address resolved across 4 mapped assets.

EVIDENCE REQUIRED

· owner type
· signer policy
· threshold
· delay windows
· emergency procedure

HIGH UNKNOWN ADMIN

Authority path unresolved - Goldoracle (Sagitta Protocol)

SCE scanned standard public authority interfaces for this asset. Current public calls did not resolve a standard owner/admin/proxy/timelock authority path. The submitted metadata identifies this asset as oracle. Verification requires source/ABI review or submitted control evidence.

CURRENT EVIDENCE STATUS

· Source: Submitted project metadata + EVM detector scan
· Contract address: 0x8A2F00Ba2E27b34d834Be83041D09632B0627056
· Admin/Owner: Unresolved
Evidence Source: Submitted project metadata + EVM detector scan
Detection Method: eth_call owner(), EIP-1967 storage slots, getOwners(), getMinDelay(), getRoleAdmin()
Detection Result: No standard owner/admin/proxy/timelock path resolved from public calls.
Confidence: unresolved
Note: Ownable owner path was not exposed; verification requires source/ABI review or submitted control evidence.
· Role: oracle

EVIDENCE REQUIRED

· owner/admin address or control model
· signer policy
· multisig or timelock address
· approval threshold
· relevant role matrix or policy document

RECOMMENDED REMEDIATION

Submit source/ABI or owner/admin evidence, identify the control model, and document multisig/timelock or governance protections for oracle authority.

LOW (4)

LOW OWNER DETECTED

On-chain owner resolved for Treasury (Sagitta Protocol)

The scanner resolved an Ownable owner from public on-chain state. This records verified control surface evidence, not a confirmed vulnerability.

CURRENT EVIDENCE STATUS

- Source: EVM detector scan — Ownable.owner()
- Contract address: 0xa4F62F8E07c85668678FDd48C2Fd982343b13687
- Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500

Evidence Source: EVM detector scan — Ownable.owner()
Detection Method: eth_call owner()
Detection Result: Ownable owner() resolved to 0xc643a9e5780420a939ced80e537f19bbe2d7c500
Confidence: verified

EVIDENCE REQUIRED

- signer policy / multisig operating procedure

RECOMMENDED REMEDIATION

Confirm whether the resolved owner is an EOA, multisig, timelock, or governed contract and document the operating procedure.

LOW OWNER DETECTED

On-chain owner resolved for Vault (Sagitta Protocol)

The scanner resolved an Ownable owner from public on-chain state. This records verified control surface evidence, not a confirmed vulnerability.

CURRENT EVIDENCE STATUS

- Source: EVM detector scan — Ownable.owner()
- Contract address: 0x30d987D24608E6D8A9A573c8B1290e2a0791356A
- Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500

Evidence Source: EVM detector scan — Ownable.owner()
Detection Method: eth_call owner()
Detection Result: Ownable owner() resolved to 0xc643a9e5780420a939ced80e537f19bbe2d7c500
Confidence: verified

EVIDENCE REQUIRED

- signer policy / multisig operating procedure

RECOMMENDED REMEDIATION

Confirm whether the resolved owner is an EOA, multisig, timelock, or governed contract and document the operating procedure.

LOW OWNER DETECTED

On-chain owner resolved for Escrow (Sagitta Protocol)

The scanner resolved an Ownable owner from public on-chain state. This records verified control surface evidence, not a confirmed vulnerability.

CURRENT EVIDENCE STATUS

- Source: EVM detector scan — Ownable.owner()
- Contract address: 0x6908b357995cFeD1008616E65Dbe428Cbd9dFA51
- Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500

Evidence Source: EVM detector scan — Ownable.owner()
Detection Method: eth_call owner()
Detection Result: Ownable owner() resolved to 0xc643a9e5780420a939ced80e537f19bbe2d7c500
Confidence: verified

EVIDENCE REQUIRED

- signer policy / multisig operating procedure

RECOMMENDED REMEDIATION

Confirm whether the resolved owner is an EOA, multisig, timelock, or governed contract and document the operating procedure.

LOW OWNER DETECTED **On-chain owner resolved for Reserve (Sagitta Protocol)**

The scanner resolved an Ownable owner from public on-chain state. This records verified control surface evidence, not a confirmed vulnerability.

CURRENT EVIDENCE STATUS

· Source: EVM detector scan — Ownable.owner()
· Contract address: 0xaf0E91C2fB084A50e2e8F207EE11468EA982a820
· Admin/Owner: 0xc643a9e5780420a939ced80e537f19bbe2d7c500
Evidence Source: EVM detector scan — Ownable.owner()
Detection Method: eth_call owner()
Detection Result: Ownable owner() resolved to 0xc643a9e5780420a939ced80e537f19bbe2d7c500
Confidence: verified

EVIDENCE REQUIRED

· signer policy / multisig operating procedure

RECOMMENDED REMEDIATION

Confirm whether the resolved owner is an EOA, multisig, timelock, or governed contract and document the operating procedure.

05 WHAT THIS MEANS

SCE scanned standard public authority interfaces for 5 mapped assets. Public calls resolved Ownable owner paths for 4 assets — Treasury (Sagitta Protocol), Vault (Sagitta Protocol), Escrow (Sagitta Protocol), Reserve (Sagitta Protocol) — all to the same owner address: 0xc643a9e5780420a939ced80e537f19bbe2d7c500. This shared owner path is the primary continuity finding in this review. Goldoracle (Sagitta Protocol) did not resolve through standard interfaces and requires source/ABI review or submitted control evidence. The resolved owner evidence does not prove a vulnerability, and it does not verify that the owner is unsafe. It means the next review gate is to confirm whether the resolved address is an EOA, multisig, timelock, or governed contract.

06 RELEVANT THREAT FAMILIES

Project relevance scores reflect categorical match strength against the case library, not exploit probability.

Admin Key / Access Control

Project relevance 99

Sagitta Protocol has 6 authority finding(s) that can make privileged access a continuity risk.

Global cases: **64** Critical (global): **64** Cases catalogued: **64**

- Freeze treasury-controlled liquidity movements and revoke suspect admin permissions
- Rotate all compromised admin keys immediately
- Enforce role separation across admin, operator, and emergency roles

Treasury / Accounting

Project relevance 64

Sagitta Protocol includes treasury movement authority, so global treasury-control incidents are directly relevant.

Global coverage: **Pending** Critical (global): **0** Cases catalogued: **0**

Global case coverage pending — relevance is based on project authority surface match, not global case history.

Governance / Quorum / Timelock

Project relevance 33

Sagitta Protocol has governance or timelock signals that affect response windows for upgrades and emergency action.

Global cases: **7** Critical (global): **5** Cases catalogued: **7**

- Revoke compromised governance keys or multisig signers
- Review and extend timelock durations for critical operations
- Activate emergency quorum policy for critical decisions

Oracle / Price Feed

Project relevance 26

Sagitta Protocol includes oracle surfaces where stale or manipulated prices can affect protocol safety.

Global coverage: **Pending** Critical (global): **0** Cases catalogued: **0**

Global case coverage pending — relevance is based on project authority surface match, not global case history.

07 RECOMMENDED CONTROLS

Controls remain grouped by asset for remediation tracking. The immediate review gate is to verify the shared owner operating model and resolve Goldoracle authority evidence; the controls below remain missing until supporting policy or governance evidence is submitted.

TREASURY CONTROLS

MISSING (6)

MISSING **Verify role separation across treasury authority surfaces**

Treasury movement, allocation, and emergency powers should be distributed across independent roles.

MISSING **Verify treasury movement authorization path**

Treasury movement authority requires a documented and verified authorization path with multisig or timelock protection.

MISSING **Document treasury allocation authority path**

Treasury allocation decisions require documented approver roles and governance path.

MISSING **Document treasury emergency pause process**

Treasury role assets require a documented emergency freeze or pause procedure with a named escalation path.

MISSING **Identify and document treasury admin/owner authorities**

Unknown admin or owner authority should be inventoried before the project can claim closure on authority risk.

MISSING **Verify multisig or timelock ownership for treasury authority**

Treasury fund movement paths should have timelock or multisig protection with documented delay windows.

VAULT CONTROLS

MISSING (6)

MISSING **Document vault deposit/withdrawal authority path**

Vault deposit and withdrawal authority requires a documented path with multisig or timelock protection.

MISSING **Document vault emergency pause process**

Vault pause authority requires a documented emergency procedure with named pause authority and unpause governance path.

MISSING **Document vault lock/unlock parameter authority**

Authority to modify vault lock or unlock parameters requires documented governance or admin path.

MISSING **Document vault upgrade authority path**

Vault upgrade authority requires a governed upgrade path with timelock and multisig protection.

MISSING **Identify and document vault admin/owner authorities**
Unknown admin or owner authority should be inventoried before the project can claim closure on authority risk.

MISSING **Verify multisig or timelock ownership for vault authority**
Vault authority surfaces with high blast radius should have timelock or multisig verification.

ESCROW CONTROLS

MISSING (6)

MISSING **Document escrow fund routing authority**
Escrow fund routing authority requires documented destination whitelists and approval paths.

MISSING **Document escrow settlement authority path**
Escrow settlement authority requires a documented path with approval thresholds and dispute resolution.

MISSING **Verify role separation across escrow authority surfaces**
Escrow settlement, routing, and batch authority should be distributed across independent roles.

MISSING **Document escrow batch finalization authority**
Batch finalization authority requires documented approval requirements and batch size limits.

MISSING **Document keeper failure and retry process for escrow**
Escrow keeper dependency requires a documented failure escalation path and fallback authority.

MISSING **Identify and document escrow admin/owner authorities**
Unknown admin or owner authority should be inventoried before the project can claim closure on authority risk.

RESERVE CONTROLS

MISSING (5)

MISSING **Document reserve asset custody and configuration authority**
Reserve asset custody and configuration authority requires a documented path with multisig or timelock protection.

MISSING **Verify role separation across reserve authority surfaces**
Reserve custody, rebalancing, and insurance parameter authority should be distributed across independent roles.

MISSING **Document reserve insurance/backstop parameter authority**
Authority to modify insurance or backstop parameters requires documented governance controls.

MISSING **Document reserve rebalance authority**
Reserve rebalance authority requires documented approval requirements and rebalance limits.

MISSING **Identify and document reserve admin/owner authorities**

Unknown admin or owner authority should be inventoried before the project can claim closure on authority risk.

ORACLE CONTROLS

MISSING (6)

MISSING **Document oracle price feed source authority**

Oracle price feed source authority requires documented update controls and source independence verification.

MISSING **Verify oracle manipulation resilience**

Oracle role assets require documented TWAP window, deviation limits, and circuit breaker configuration.

MISSING **Document oracle update/configuration authority**

Oracle configuration authority requires documented governance path with timelock and multisig protection.

MISSING **Identify and document goldoracle admin/owner authorities**

Unknown admin or owner authority should be inventoried before the project can claim closure on authority risk.

MISSING **Verify oracle fallback/stale-price policy**

Fallback oracle authority requires documented circuit breaker configuration and trigger conditions.

MISSING **Verify oracle stale-price policy**

Oracle stale price handling requires documented heartbeat thresholds and fallback behavior.

08 VERIFICATION STATUS

CONTROLS TOTAL	CONTROLS VERIFIED	COVERAGE	OWNER EVIDENCE OBSERVED	AUTHORITY PATHS RESOLVED	AUTHORITY PATHS AWAITING
29	0 / 29	0%	4 / 5	4 / 5	1 / 5

COVERAGE INCOMPLETE

0 of 29 evidence and control checks verified (0% coverage). "Defended" status applies only when all checks are verified against current project metadata and evidence.

09 NEXT ACTIONS

1. Confirm whether 0xc643a9e5780420a939ced80e537f19bbe2d7c500 is an EOA, multisig, timelock, or governed contract.

2. Provide signer policy, threshold, delay windows, and emergency procedure for the shared owner.
3. Resolve Goldoracle (Sagitta Protocol) authority path through source/ABI review or submitted control evidence.
4. Verify whether critical powers should remain concentrated or be split across multisigs, timelocks, or governed roles.
5. Submit supporting policy evidence and re-run SCE Admin Surface Scan.
6. Generate updated report with verified-control coverage. Current status: 0 of 29 evidence and control checks verified.