

Oct. 22, 2025

Presented by:

k66, Emily, Jack
@SuiAudit Lab

SuiAudit

AI-Powered Sui-Move Audit Solution



3rd place@2025 Sui Taipei Dev Hackathon

鏈上資安有多重要？開始前先說個故事...

2025-05-22

Cetus
Protocol

約 2.23 億美元

當天幣價跌
80%

Sui 台北黑客松
09-14

2025-09-07

Nemo
Protocol

約 240 萬美元

Sui HOH 黑客松
10-22

2025-10-15

Typus
Finance

約 340 萬美元



鏈上資安超重要！但傳統審計服務又貴又慢！

於是 SuiAudit 誕生了！

The image shows a composite screenshot of the SuiAudit platform. On the left, a large blue header bar contains the SuiAudit logo. Below it, a green button says "All systems operational". A central blue box is labeled "Featured" and contains the "AI-Powered Sui-Move Code Audit" section. This section includes a brief description: "Comprehensive smart contract security analysis powered by advanced AI. Detect vulnerabilities and ensure code quality.", a "Start Audit" button, and a "Blocklist Detection" link below it. To the right, there's a "Protected" status indicator and a "Sui-Move Code Audit" result for package ID 0xe14726c336e81b32328e92afc37345d1591, dated 2025-10-20 at 05:15:13. The audit was successful ("Pass SuiAudit"). At the bottom, a large callout bubble states "SuiAudit = Sui + AI Code Audit".

SuiAudit

All systems operational

Featured

AI-Powered Sui-Move Code Audit

Comprehensive smart contract security analysis powered by advanced AI. Detect vulnerabilities and ensure code quality.

Start Audit

Blocklist Detection

Protected

Blocklist Detection

Website Security Checker

Sui-Move Version Validator

Blocklist Report

Pass SuiAudit

Package ID:
0xe14726c336e81b32328e92afc37345d1591

批准 - 檢測到低風險 (ML+規則引擎)

Audit Time: 2025-10-20 05:15:13

查看 NFT 證書

SuiAudit = Sui + AI Code Audit

AUDIT REPORTS

The severity levels assigned to findings categorize them based on their potential impact and likelihood, helping to prioritize remediation efforts.



Description	Description
High	Vulnerabilities that can result in a direct loss of funds, asset control, or critical system failure.
Medium	Issues that may lead to unexpected behavior or potential exploits and should be addressed before deployment.
Low	Deviations from best practices that pose minor risks or negatively impact future code maintainability.
Informational	Auditor notes, code quality suggestions, or points of interest highlighted for special attention.

AI MODEL RESULT

Table 1. Benchmark test results

Platform	Projects
Aptos	did-aptos, jujube_tool, koiz-contracts, LayerZero-Aptos-Contract
Starcoin	FAI, poly-stc-contracts
Sui	basic-coin, cetus-amm, defi, Dmens, fungible_tokens, integer-mate, nft-protocol, nfts, object-market, originmate, poly-stc-contracts, pyth-crosschain-sui, suia, Sui-AMM-swap, sui-red-packet, wormhole

In the benchmark dataset, the evaluation of MoveScanner's vulnerability detection shows that the processing time ranges from 12.1 ms to 217.5 ms, with an average of 63.2 ms per module. The results indicate that MoveScanner performs particularly well in detecting resource leaks and arithmetic overflow vulnerabilities, which aligns with the implementation focus. The detection performance for various types of vulnerabilities is summarized in the Tab 2.

Vulnerability Type	Test Cases	Detected	Detection Rate (%)	False Positives	False Positive Rate (%)
Resource Leak	8	4	50	0	0
Arithmetic Overflow	5	3	60	0	0
Unchecked Return	7	9	100	0	0
Cross-Module Pollution	4	4	100	0	0
Capability Leak	10	10	100	0	0
Total	34	30	88.2	0	0

Table 2. Benchmark test results

Vulnerability Type	MoveScanner	SuiAudit
Resource Leak	50% (=4/8)	72.7% (=8/11)
Arithmetic Overflow	60% (=3/5)	100% (=11/11)
Unchecked Return	100% (=9/7)	100% (=11/11)
Cross-Module Pollution	50% (=4/8)	100% (=11/11)
Capability	100% (=10/10)	100% (=11/11)
No significant vulnerabilities	N/A	72.7% (=8/11)
Total	88% (=30/34)	92.4% (=61/66)

EXECUTION

```
PROBLEMS 8 OUTPUT DEBUG CONSOLE TERMINAL PORTS  
stral_66samples.log  
Setting `pad_token_id` to `eos_token_id`:2 for open-end generation.  
(venv) k66@k66:~/suiguard/backend$ sleep 600 && cd /home/k66/suiguard/backend && tail -100 test_mistral_66samples.log | tail -40  
[1]+ Done cd /home/k66/suiguard/backend && source venv/bin/activate && nohup python test_all_samples.py > test_mistral_66samples.log 2>&1  
✓ 樣本 53/66 | 相似度: 100% | 時間: 30.65s | Cross-Module Pollution  
✓ 樣本 54/66 | 相似度: 90% | 時間: 30.04s | Cross-Module Pollution  
✓ 樣本 55/66 | 相似度: 90% | 時間: 30.22s | Cross-Module Pollution  
✓ 樣本 56/66 | 相似度: 90% | 時間: 29.31s | Cross-Module Pollution  
✓ 樣本 57/66 | 相似度: 80% | 時間: 29.96s | Capability Leak  
✓ 樣本 58/66 | 相似度: 90% | 時間: 30.18s | Capability Leak  
✓ 樣本 59/66 | 相似度: 90% | 時間: 30.28s | Capability Leak  
✓ 樣本 60/66 | 相似度: 80% | 時間: 30.21s | Capability Leak  
✓ 樣本 61/66 | 相似度: 80% | 時間: 30.70s | Capability Leak  
✓ 樣本 62/66 | 相似度: 100% | 時間: 30.88s | Capability Leak  
✓ 樣本 63/66 | 相似度: 80% | 時間: 31.88s | Capability Leak  
✓ 樣本 64/66 | 相似度: 90% | 時間: 33.86s | Capability Leak  
✓ 樣本 65/66 | 相似度: 80% | 時間: 30.71s | Capability Leak  
✓ 樣本 66/66 | 相似度: 90% | 時間: 25.69s | Capability Leak  
=====  
■ 測試結果總結  
=====  
總樣本數: 66  
有效樣本: 66  
✓ 正確數量: 61  
✗ 錯誤數量: 5  
準確率: 92.4%  
平均相似度: 81.1%  
平均推理時間: 29.67 秒  
總推理時間: 1958.46 秒  
=====  
■ 按漏洞類型分析  
=====  
Arithmetic Overflow: 11/11 (100.0%)  
Capability Leak: 11/11 (100.0%)  
Cross-Module Pollution: 11/11 (100.0%)  
Resource Leak: 9/11 (81.8%)  
Unchecked Return: 11/11 (100.0%)  
未發現明顯漏洞: 8/11 (72.7%)  
=====  
✓ 詳細結果已保存到: test_results_mistral.json  
=====  
(venv) k66@k66:~/suiguard/backend$ []
```

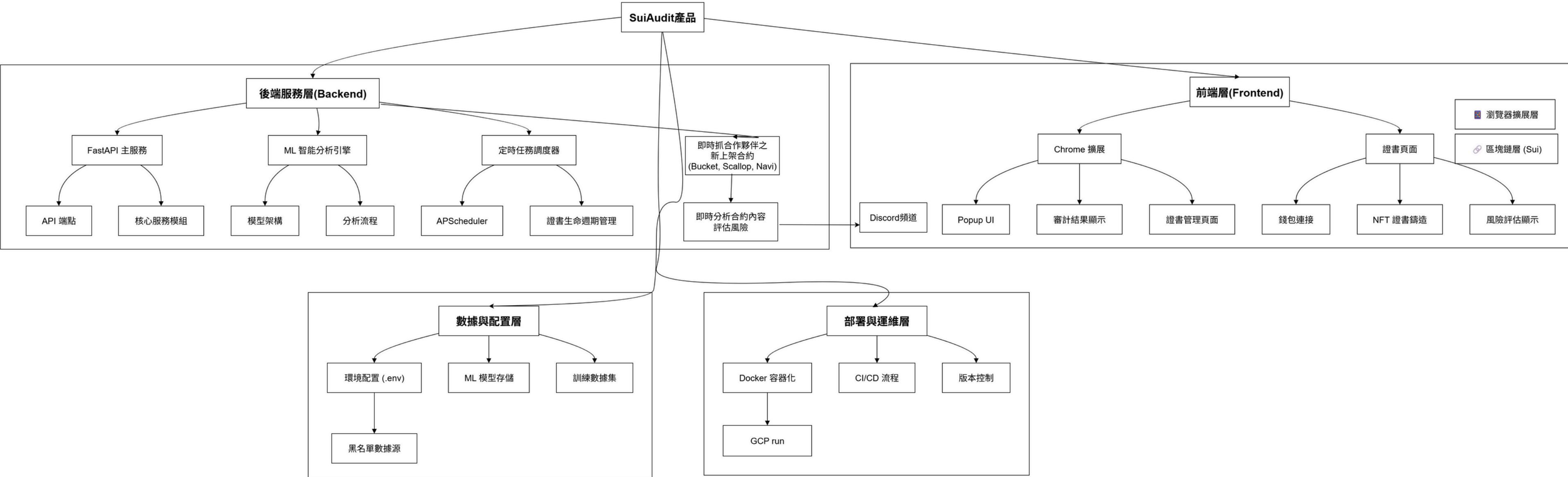
SUIAUDIT WILL CHALLENGE THEM!

Sui Move & MoveEVM's Paper:

1. [2018 Luo] "MoveScanner: Analysis of Security Risks of Move Smart Contracts",
<https://arxiv.org/html/2508.17964v1>
2. [2025 Topal] "A Systematic Classification of Vulnerabilities in MoveEVM Smart Contracts (MWC)"
,<https://arxiv.org/pdf/2505.19047.pdf>
3. [Tang 2023] "Deep learning-based solution for smart contract vulnerabilities detection",
<https://www.nature.com/articles/s41598-023-47219-0>
4. [Luo 2025] "MoveScanner: Analysis of Security Risks of Move Smart Contracts" ,
<https://arxiv.org/html/2508.17964v1>
5. [龔2025] "基于智能合约漏洞检测的元模型算法", https://pdf.hanspub.org/csa2025152_101543498.pdf
6. [Liu 2024] "PropertyGPT: LLM-driven Formal Verification of Smart Contracts through Retrieval-Augmented Property Generation", <https://arxiv.org/pdf/2405.02580>

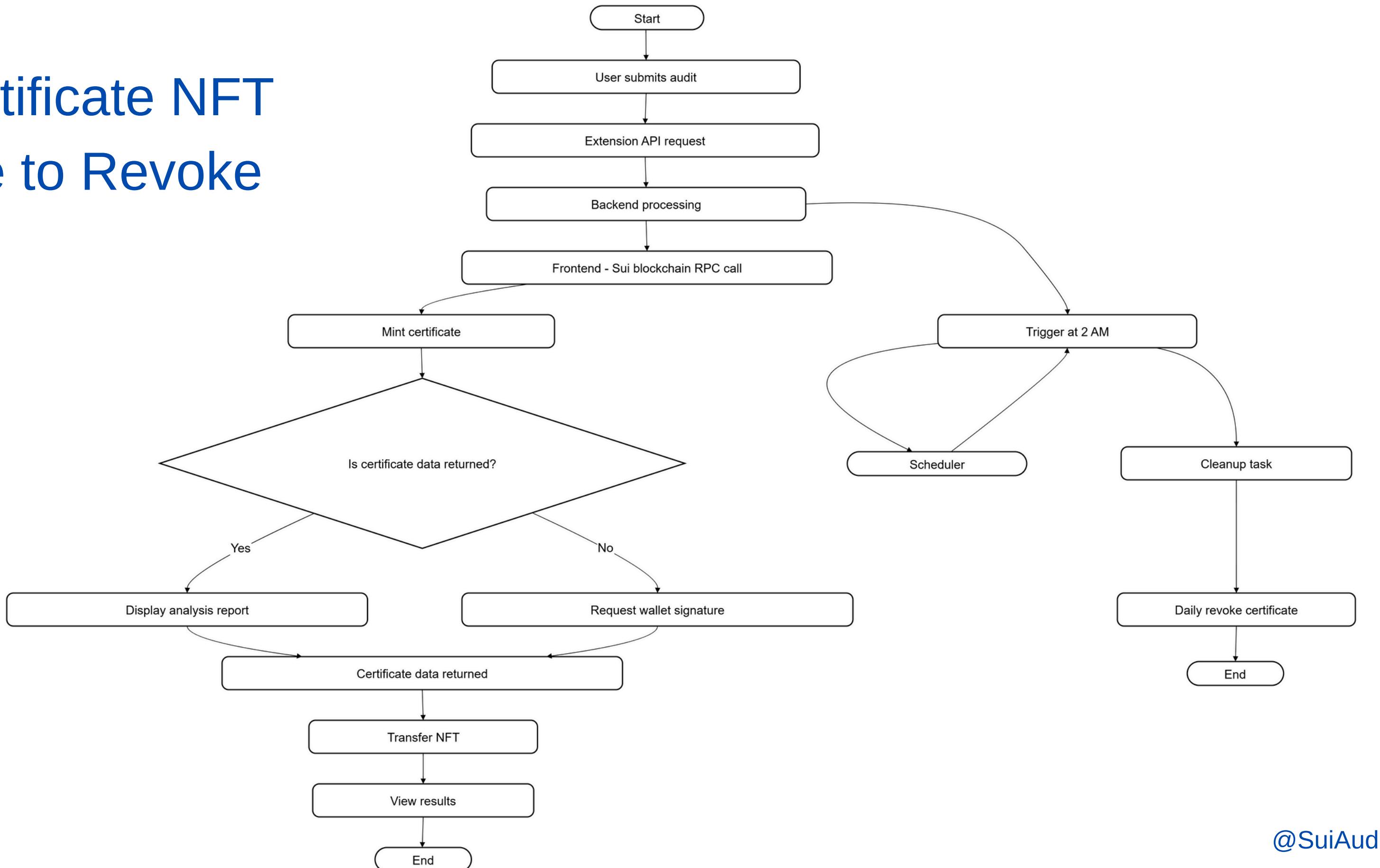
We(SuiAudit Lab) host study & dev syncup meet weekly via Discord.
And next step we will host livesteam meet via Youtube, X.

SYSTEM ARCHITECTURE(1/2)

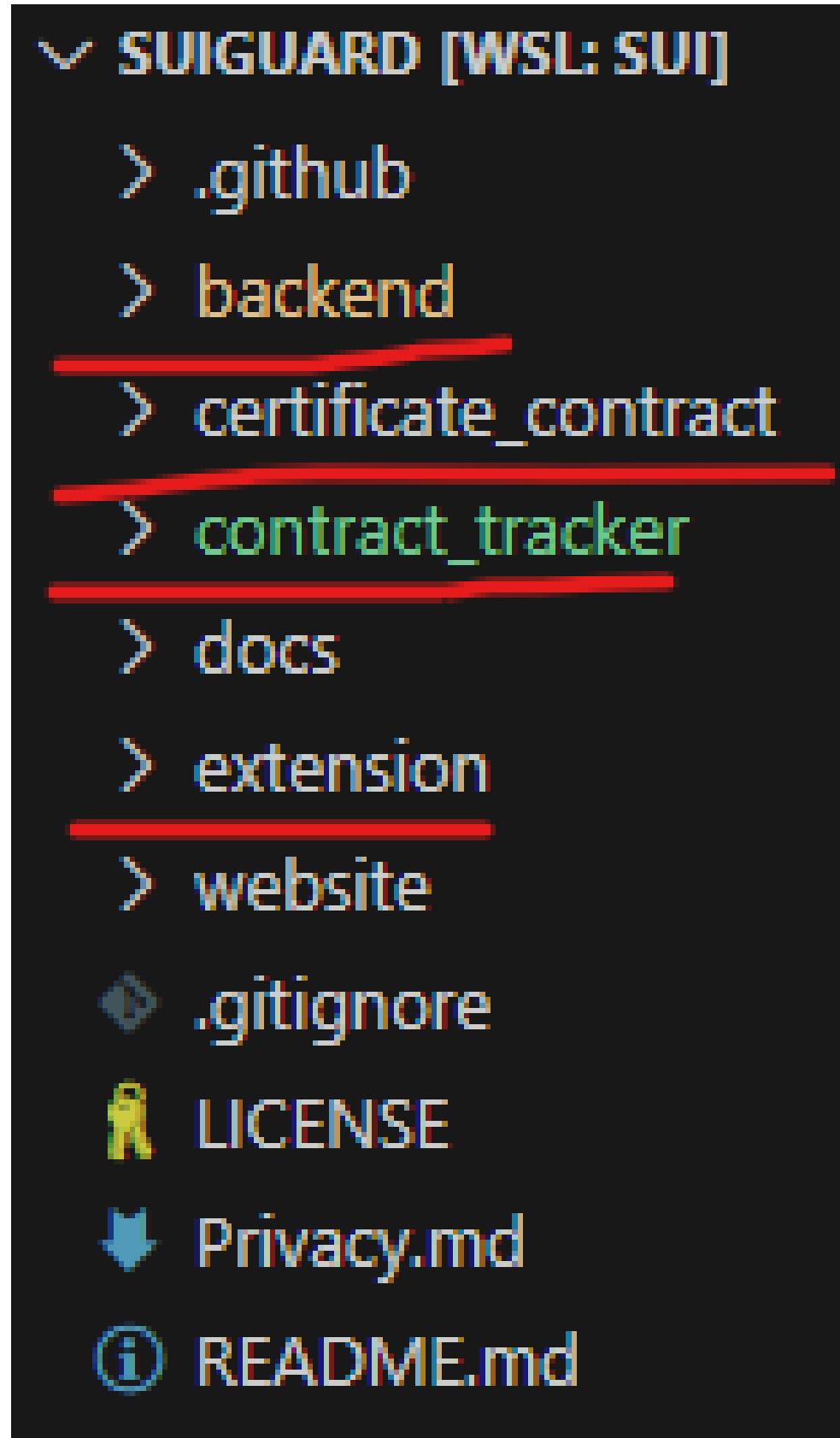


SYSTEM ARCHITECTURE(2/2)

SuiAudit certificate NFT from Create to Revoke



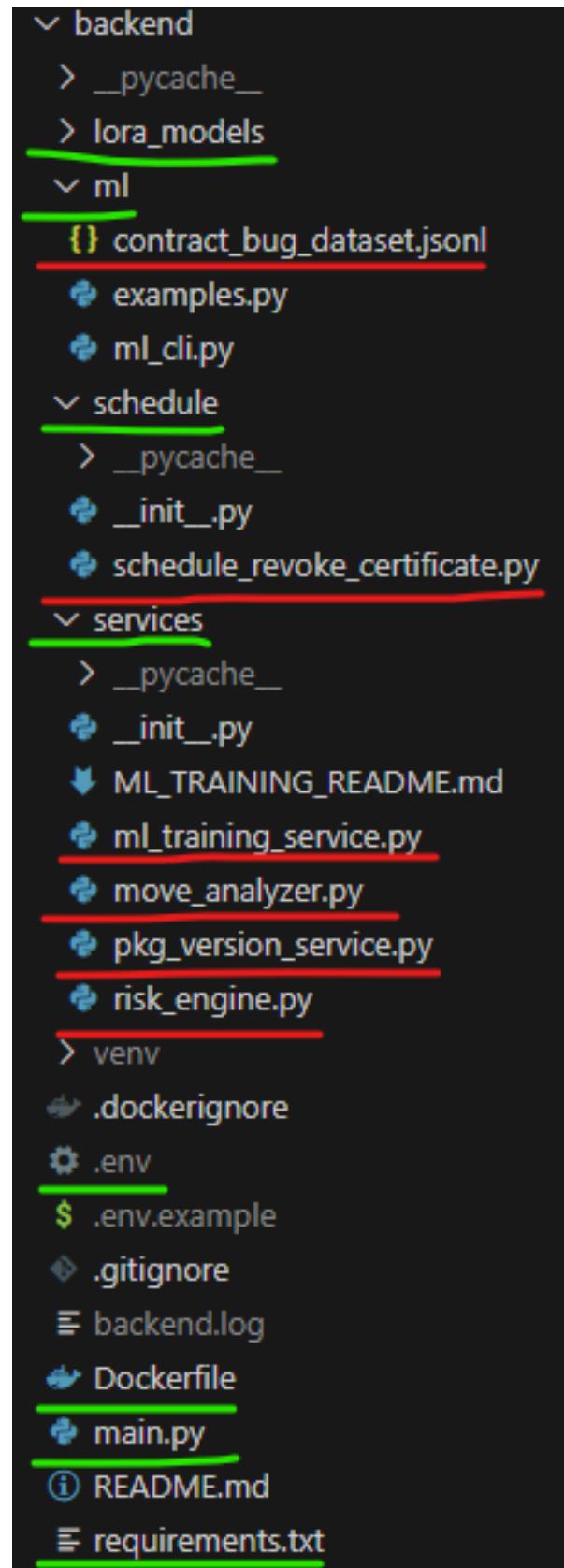
CODE DETAILS(1/4)



git clone:
<https://github.com/k66inthesky/suiguard>

1. 後端 - backend/ 主運算邏輯
2. 後端 - contract_trader/ 即時抓合作夥伴之新上架合約，並發布風險訊號至Discord
3. 前端 - extension/ 插件前端
4. 智能合約 - certificate_contract/

CODE DETAILS(2/4)



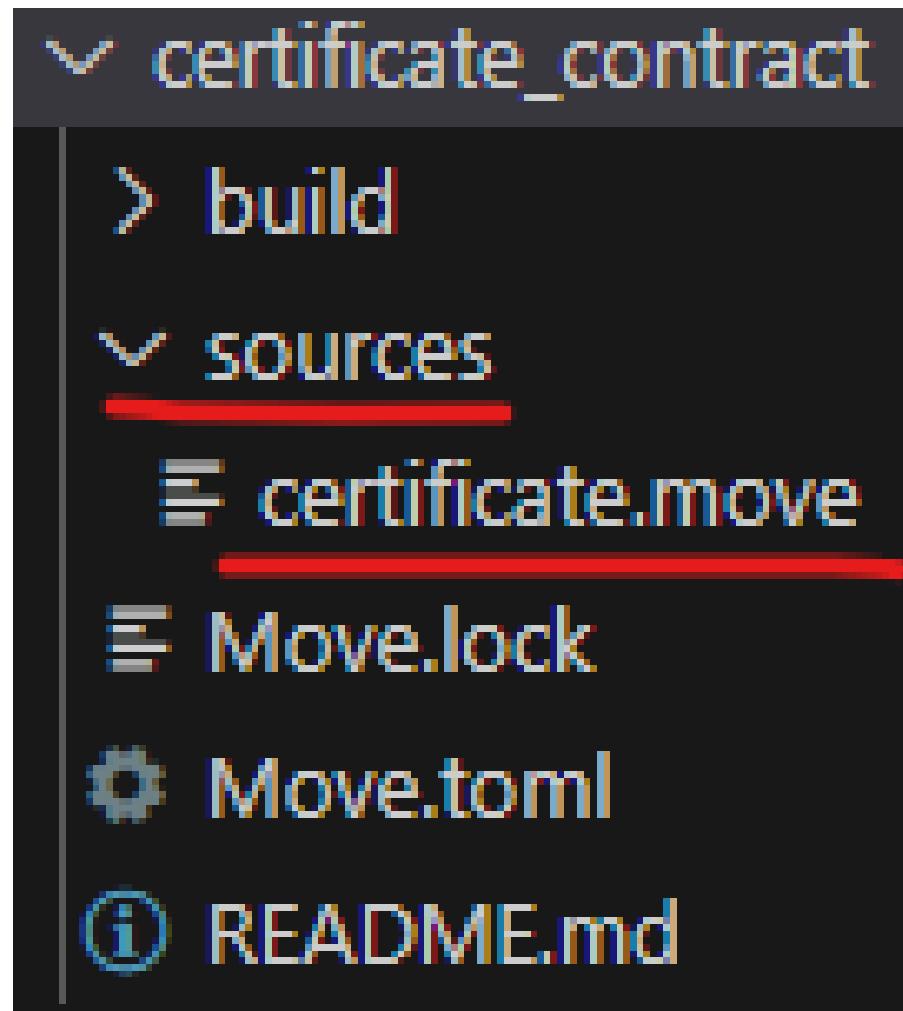
後端 - backend/

1. main.py 程式入口點
2. lora_models/ 放權重(推理會被載入)與checkpoint-27/(僅訓練時需)
3. ml/contract_bug_dataset.jsonl 訓練集
4. schedule/schedule_revocate_certificate.py 定期撤回過期NFT證書
5. services/
 - |---move_analyzer.py 將智能合約解構+正則
 - |---ml_training.py ML訓練
 - |---risk_engine.py 結合以上，綜合引擎去計算風險分數
 - |---pkg_version_service.py 合約版本檢查
6. .env (.env.example)設定檔
7. venv/ 及 Dockerfile 安裝方式可選這兩種之一

CODE DETAILS(3/4)

智能合約

move - certificate_contract/



```
certificate_contract > sources > certificate.move
3  module suiguard_certificate::certificate {
4    use sui::object::{Self, UID};
5    use sui::transfer;
6    use sui::tx_context::{Self, TxContext};
7    use std::string::{Self, String};
8    use sui::clock::{Self, Clock};
9    use sui::event;
10
11   /// Error codes
12   const ENotExpired: u64 = 1;
13   const EUnauthorized: u64 = 2;
14
15   /// Admin capability for managing certificates
16   > public struct AdminCap has key, store { ... }
17
18
19
20   /// Security Certificate NFT for audited Sui packages
21   > public struct SecurityCertificate has key, store { ... }
22
23
24   /// Certificate issued event
25   > public struct CertificateIssued has copy, drop { ... }
26
27
28   /// Certificate revoked event
29   > public struct CertificateRevoked has copy, drop { ... }
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50   /// Initialize the module - creates admin capability
51   > fun init(ctx: &mut TxContext) { ... }
52
53
54
55
56
57   /// Issue a new security certificate for an audited package
58   /// User pays gas fee to mint their certificate
59   > public entry fun issue_certificate(...
60
61
62
63
64
65
66
67
68   ) { ... }
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96   /// Get certificate details
97   > public fun get_certificate_info(cert: &SecurityCertificate): (String, String, u8, u64, u64)
98
99
100
101
102
103
104
105
106
```

CODE DETAILS(4/4)

```
certificate_contract > sources > certificate.move
58     /// User pays gas fee to mint their certificate
59     public entry fun issue_certificate(
60         recipient: address,
61         package_id: vector<u8>,
62         risk_level: vector<u8>,
63         security_score: u8,
64         recommendation: vector<u8>,
65         analyzer_version: vector<u8>,
66         clock: &Clock,
67         ctx: &mut TxContext
68     ) {
69
70         let current_time: u64 = clock::timestamp_ms(clock: clock);
71         let expiry_time: u64 = current_time + (30 * 24 * 60 * 60 * 1000); // 30 days validity
72
73         let certificate: SecurityCertificate = SecurityCertificate {
74             id: object::new(ctx: ctx),
75             recipient,
76             package_id: string::utf8(bytes: package_id),
77             risk_level: string::utf8(bytes: risk_level),
78             security_score,
79             certification_date: current_time,
80             expiry_date: expiry_time,
81             recommendation: string::utf8(bytes: recommendation),
82             analyzer_version: string::utf8(bytes: analyzer_version),
83         };
84
85         // Emit certificate issued event
86         event::emit(event: CertificateIssued {
87             certificate_id: object::id(obj: &certificate),
88             recipient,
89             package_id: string::utf8(bytes: package_id),
90             security_score,
91             risk_level: string::utf8(bytes: risk_level),
92         });
93
94         transfer::public_transfer(obj: certificate, recipient: recipient);
95     }
```

certificate_contract/source/ certificate.move

```
certificate_contract > sources > certificate.move
112     /// Revoke certificate (burn it) - user can revoke their own certificate
113     public entry fun revoke_certificate(cert: SecurityCertificate) { ...
114     }
115
116     /// Admin burns expired certificate
117     public entry fun burn_expired_certificate(
118         _admin: &AdminCap,
119         cert: SecurityCertificate,
120         clock: &Clock,
121     ) {
122         // Verify certificate is expired
123         assert!(!is_valid(cert: &cert, clock: clock), ENotExpired);
124
125         let SecurityCertificate { id: UID, recipient: address, package_id: String, .. } = cert;
126
127         event::emit(event: CertificateRevoked {
128             certificate_id: object::uid_to_inner(uid: &id),
129             recipient,
130             package_id,
131             revoke_reason: string::utf8(bytes: b"expired"),
132         });
133
134         object::delete(id: id);
135     }
136
137 }
```

TRANSACTION ON SUI TESTNET(1/2)

The screenshot shows a web browser window with the URL <https://testnet.suivision.xyz/package/0xfa3e12bc4632fc5b4c8bb0e39255c22a2e09d93657a5a7f8206b347e526b8a45>. The page title is "Package". The main content area displays the following details:

Details
Publisher: 0x876f...4b5f
Publish Time: Oct 17, 2025 20:42:27 +UTC
Last Transaction ID: C2Hi1mBaTsFFAS5jfNUSBKMzLkhoT973xrr4gth5KRPU
Version: 1
Owner: Immutable

Below this, there are tabs for "Transaction Blocks", "Code", and "Statistics". The "Transaction Blocks" tab is selected, showing a table of transaction blocks:

DIGEST	PAYLOAD	SENDER	TXNS	STATUS	AGE	GAS
BLChAB...1PsV	0xfa3e...8a45::certificate::issue_...cate	0x5c33...7bae	1	✓	35 mins 20 secs ago	-0.00307816 SUI
5crGp4...tthu	0xfa3e...8a45::certificate::issue_...cate	0xfcfc6...f875	1	✓	1 day 2 hrs ago	0.00376868 SUI
9DWsZM...NTCK	0xfa3e...8a45::certificate::issue_...cate	0xfcfc6...f875	1	✓	1 day 3 hrs ago	0.00376868 SUI

At the bottom right of the page, there is a watermark-like text: "@SuiAudit Lab".

package_id:
0xfa3e12bc4632fc5b4c8bb0e39255c22a2
e09d93657a5a7f8206b347e526b8a45

TRANSACTION ON SUI TESTNET(2/2)

testnet.suivision.xyz/txblock/BLCnABtj5s5ZGyYvmtRmLH6Ap6ehw81FfK5H1QNG1PsV?tab=Overview

SuiVision Blockchain ▾ Validators

Transaction Block

BLCnAB...1PsV

Overview Changes Events (1) User Signatures Raw JSON

Checkpoint:	254,415,340
Timestamp:	38 mins 59 secs ago (Oct 19, 2025 13:18:25 +UTC)
Sender:	0x5c33...7bae
Recipients:	0x5c33...7bae
Status:	Success
Amount:	0 (0 MIST)

Total Gas Fee: -0.00307816 (-3,078,160 MIST)

Computation Fee: 0.001 (1,000,000 MIST)

Storage Fee: 0.0037468 (3,746,800 MIST)

Storage Rebate: 0.00782496 (7,824,960 MIST)

Gas Payment: 0x256767efdc7cfb436986e0e29a2d2ee79b78587f3a2cf47b29071ecc72d5acf5

Gas Budget: 0.0057468 (5,746,800 MIST)

Gas Price: 0.000001 (1,000 MIST)

testnet.suivision.xyz/txblock/BLCnABtj5s5ZGyYvmtRmLH6Ap6ehw81FfK5H1QNG1PsV?tab=Overview

Inputs: **RAW**

```
[  
  0: {  
    type: "pure"  
    valueType: "address"  
    value: "0x5c330784e7a4d295bbb9f24dd965ce83b823f37de8600fdfc4e241ce66f07bae"  
  },  
  1: {  
    type: "pure"  
    valueType: "vector<u8>"  
    value: "0xe14726c336e81b32328e92afc37345d159f5b550b09fa92bd43640cfdd0a0cfcd"  
  },  
  2: {  
    type: "pure"  
    valueType: "vector<u8>"  
    value: "LOW"  
  },  
  3: {  
    type: "pure"  
    valueType: "u8"  
    value: 0  
},  
  4: {  
    type: "pure"  
    valueType: "vector<u8>"  
    value: "批准 - 檢測到低風險 (ML+規則引擎)"  
},  
]
```

Click to See More ↓

Transactions & Inputs: **RAW**

```
[  
  0: {  
    MoveCall: {  
      package: "0xfa3e12bc4632fc5b4c8bb0e39255c22a2e09d93657a5a7f8206b347e526b8a45"  
      module: "certificate"  
      function: "issue_certificate"  
      arguments: [...]  
    }  
  },  
]
```

TESTNET TX BLOCK

→ G testnet.suivision.xyz/txblock/BLCnABtj5s5ZGyYvmtRmLH6Ap6ehw81FfK5H1QNG1PsV?tab=Overview

SuiVision Blockchain ▾ Validators

Transaction Block BLCnAB...1PsV

Overview Changes Events (1) User Signatures Raw JSON

package_id:
0xfa3e12bc4632fc5b4c8bb0e
39255c22a2e09d93657a5a7f8
206b347e526b8a45

Checkpoint: 254,415,340

Timestamp: 38 mins 59 secs ago (Oct 19, 2025 13:18:25 +UTC)

Sender: 0x5c33...7bae

Recipients: 0x5c33...7bae

Status: Success

Amount: 0 ⚡ (0 MIST)

Total Gas Fee: -0.00307816 ⚡ (-3,078,160 MIST)

Computation Fee: 0.001 ⚡ (1,000,000 MIST)

Storage Fee: 0.0037468 ⚡ (3,746,800 MIST)

Storage Rebate: 0.00782496 ⚡ (7,824,960 MIST)

Gas Payment: 0x256767efdc7cfb436986e0e29a2d2ee79b78587f3a2cf47b29071ecc72d5acf5

Gas Budget: 0.0057468 ⚡ (5,746,800 MIST)

Gas Price: 0.000001 ⚡ (1,000 MIST)

Transaction Blocks Code Statistics

Transaction Blocks

Updated Objects **Input Objects**

DIGEST	PAYLOAD
2iJrxR...FWVF	0xfa3e...8a45::certificate::issue_...cate
BLCnAB...1PsV	-
5crGp4...tthu	-
9DWsZM...NTCk	-

SCALLOP, NAVI, BUCKET PKG ALERT BOT

SuiAudit Lab # bucket-alerts

自下午4:07以來有2則新訊息 標示為已讀

歡迎來到 #bucket-alerts !

這就是 #bucket-alerts 頻道的起點。

2025年10月22日 新的

SuiAudit Monitor 應用 下午4:07

新合約檢測 - BUCKET
檢測到新的bucket協議合約部署

Package ID
0x155a2b4a924288070dc6cced78e6af9e244c654294a9863aa4b4544ccdedcb0f

部署者
0xce7c4460ee50d5c1bb1d7d5c1e4a3b9c3e9c6e7a2f1d3b5e8c4f7a1e3 BUCKET
c6d9b2

協議

Transaction
查看詳情

SuiAudit Package Monitor · 今天下午4:07

SuiAudit Risk Analyzer 應用 下午4:07

風險分析報告 - BUCKET
檢測到 bucket 協議合約的安全風險

Package ID
0x155a2b4a924288070dc6cced78e6af9e244c654294a9863aa4b4544ccdedcb0f

風險評分
92/100 (CRITICAL)

置信度
85.5%

分析方法
ML_ANALYSIS

member - 2

emily PPLX

k66 SUI 不會主動私你，私你必為詐騙！

線上 - 1

pawa 應用 正在聽 2.15.1 | https://pawa.im

離線 - 1

JackTsai HF

SuiAudit Monitor 應用 下午4:07

新合約檢測 - NAVI
檢測到新的navi協議合約部署

Package ID
0xd899cf7d2b5db716bd2cf55599fb0d5ee38a3061e7b6bb6eebf73fa5bc4c81ca
8c1

部署者
0xle4f7a0d3e6b9c2f5a8e1b4d7c0a3f6e9b2d5c8f1a4b7e0c3d6f9a2e5b NAVI

協議

Transaction
查看詳情

SuiAudit Package Monitor · 今天下午4:07

SuiAudit Risk Analyzer 應用 下午4:08

風險分析報告 - NAVI
檢測到 navi 協議合約的安全風險

Package ID
0xd899cf7d2b5db716bd2cf55599fb0d5ee38a3061e7b6bb6eebf73fa5bc4c81ca
8c1

風險評分
92/100 (CRITICAL)

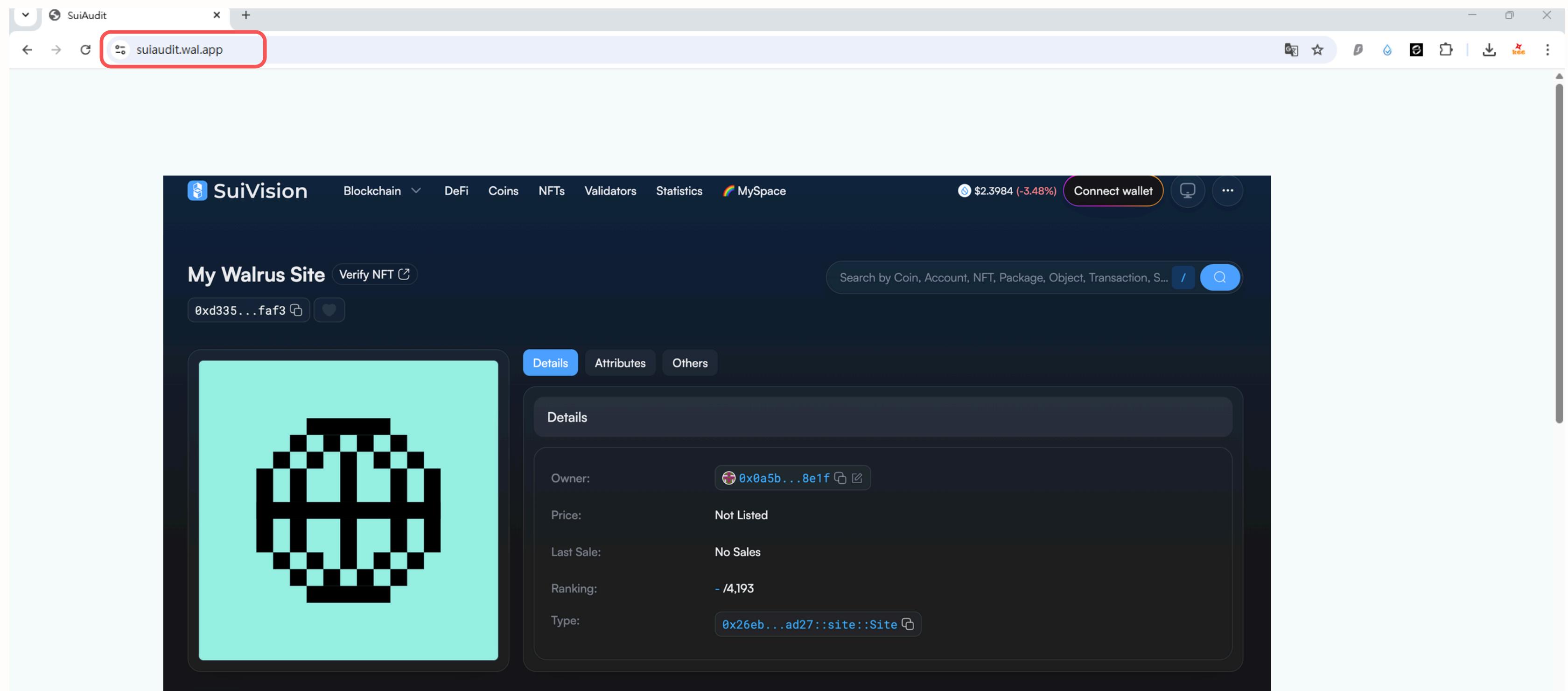
置信度
85.5%

分析方法
ML_ANALYSIS

發現的漏洞
• Potential reentrancy vulnerability in lending functions

安全問題
• Missing input validation on critical parameters
• Potential integer overflow in calculation functions

WALRUS SITE MAINNET DEPLOY



ISO STATUS UPDATE

ISO 27001 is an internationally recognized information security management standard and a key certification for assessing audit firms and trusting an organization's information security capabilities.



Control Category	Number of Controls	Progress	Key Focus Areas
Organizational Controls	37	19/37	Leadership & Governance, Risk Management, Supplier Relationships, Incident Management
People Controls	8	5/8	Training & Awareness, Accountability, Secure Remote Work
Physical Controls	14	3/14	Environmental Security, Access Management, Equipment Protection
Technological Controls	34	15/34	Secure Systems, Secure Development, Data Protection
Total	93	42/93	Four Major Control Areas

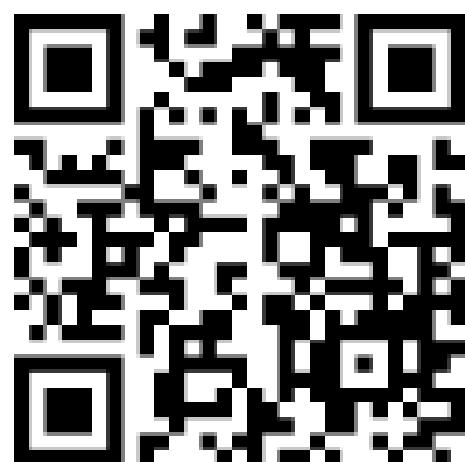
SuiAudit的商業模型有2種

MEET OUR TEAM

k66



Backend, ML, System Design



Emily



Frontend, UI/UX, System Design



Jack

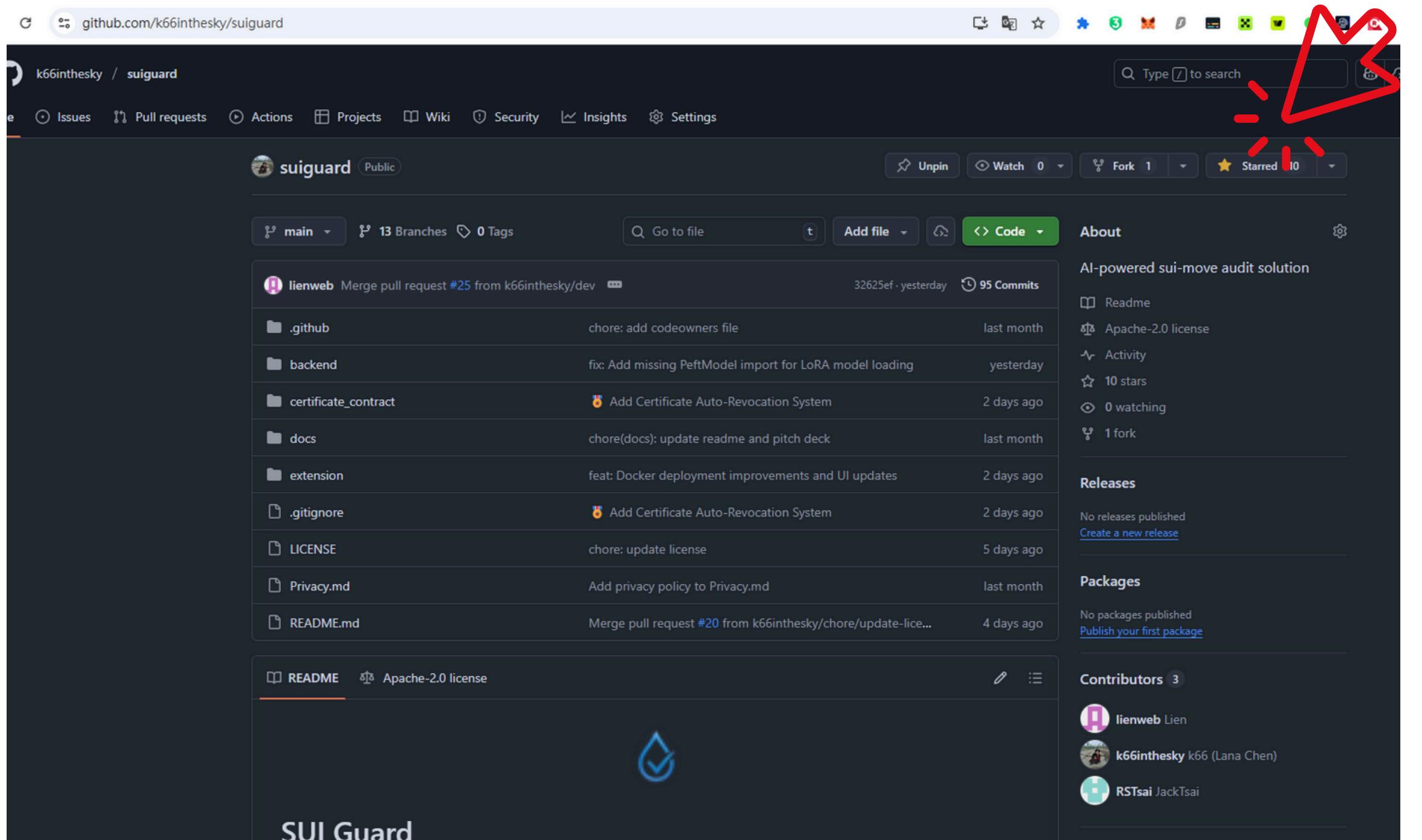


Data Analyst



ABOUT SUIAUDIT LAB

<https://github.com/k66inthesky/suiguard>



The screenshot shows the GitHub repository page for `suiguard`. The repository is public and has 95 commits. The main branch is `main`, which has 13 branches and 0 tags. The repository has 10 stars and 1 fork. The README file is visible, and the license is Apache-2.0. Contributors listed are `lienweb`, `k66inthesky`, and `RSTsai`.

Commits

- lienweb Merge pull request #25 from k66inthesky/dev 32625ef · yesterday 95 Commits
- .github chore: add codeowners file last month
- backend fix: Add missing PeftModel import for LoRA model loading yesterday
- certificate_contract 🚨 Add Certificate Auto-Revocation System 2 days ago
- docs chore(docs): update readme and pitch deck last month
- extension feat: Docker deployment improvements and UI updates 2 days ago
- .gitignore 🚨 Add Certificate Auto-Revocation System 2 days ago
- LICENSE chore: update license 5 days ago
- Privacy.md Add privacy policy to Privacy.md last month
- README.md Merge pull request #20 from k66inthesky/chore/update-lice... 4 days ago

README Apache-2.0 license

SUIGuard

