

Sep. 14, 2025
Presented by:
k66

SUI GUARD

Real-time Security Extension for SUI Users

SuiGuard got 3rd place at 2025 Sui Taipei Hackathon





WHY IS THIS IMPORTANT?

2025.02 Bybit was hacked \$1.5B

2025.05 Cetus was hacked \$0.22B

2025.09 Nemo Protocol was hacked \$2.4M



AI CODING TODAY

People used AI coding, and it comes some problem...

Ownership
unclear

logic error

Maintenance
difficulty

Security
risks

Code
quality
issues

Intellectual
property
concerns

Hidden
bugs

DEMO VIDEO

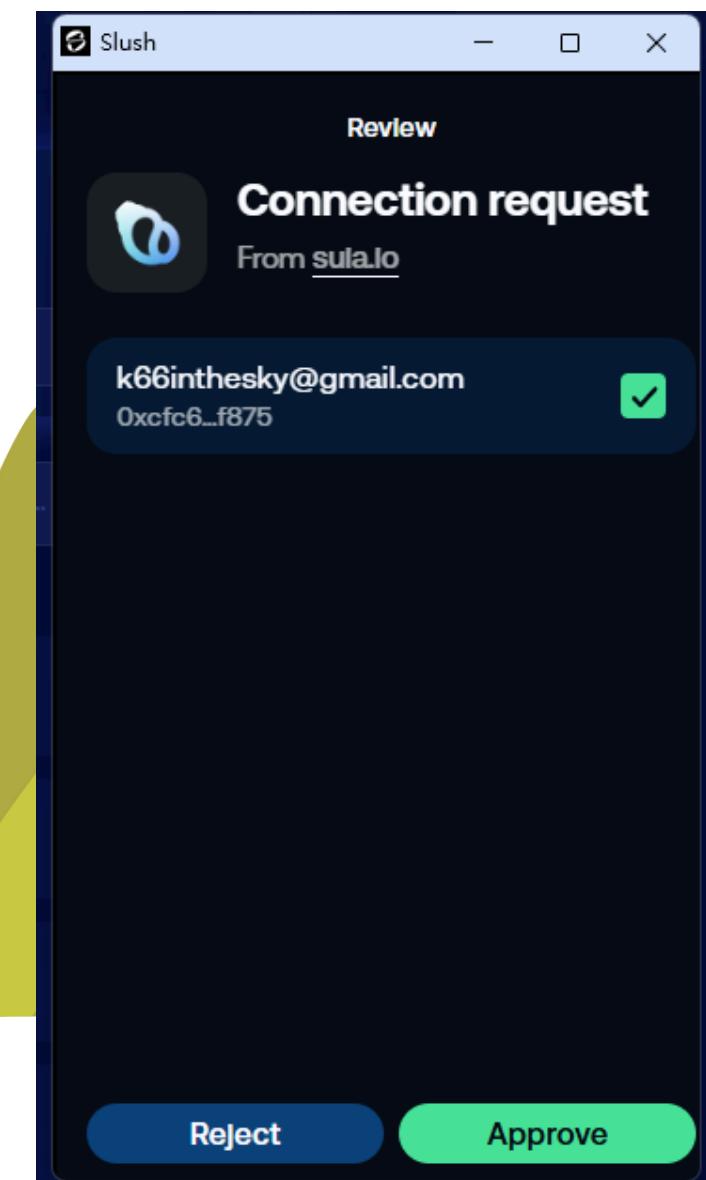
The image shows a split-screen view. On the left is the official Suia.io website, which features a dark blue header with the logo and the text "Turns your X into a AgentX". Below this is a "How It Works" section with three numbered steps:

- 1 Drop any X profile link and create a AgentX. FCFS.
- 2 BUY/SELL at any time to lock in your profits or losses.
- 3 When bonding curve reaches a market cap of \$12k (≈ 5679 SUI), all the liquidity is then deposited in Cetus and burned.

The footer of the website includes a disclaimer: "Suia.io is an ongoing social experiment, NOT an investment, security, or form of equity."

On the right is a separate window titled "網站安全性查詢" (Website Security Query) with the URL "https://suia.io/" entered. The results show a red warning icon and a risk score of "風險評分: 90". A legend at the bottom defines the colors: green for trusted sites, yellow for medium-risk sites, and red for high-risk sites. The window is signed off by "Made by SuiGuard Team".

AIRDROP HUNTER'S ONE DAY LIFE



WHAT DOES SUIGUARD DO?

Sui Guard offers 3 core features.



REAL-TIME BLACKLIST UPDATE
(WEB3 WHOSCALL)



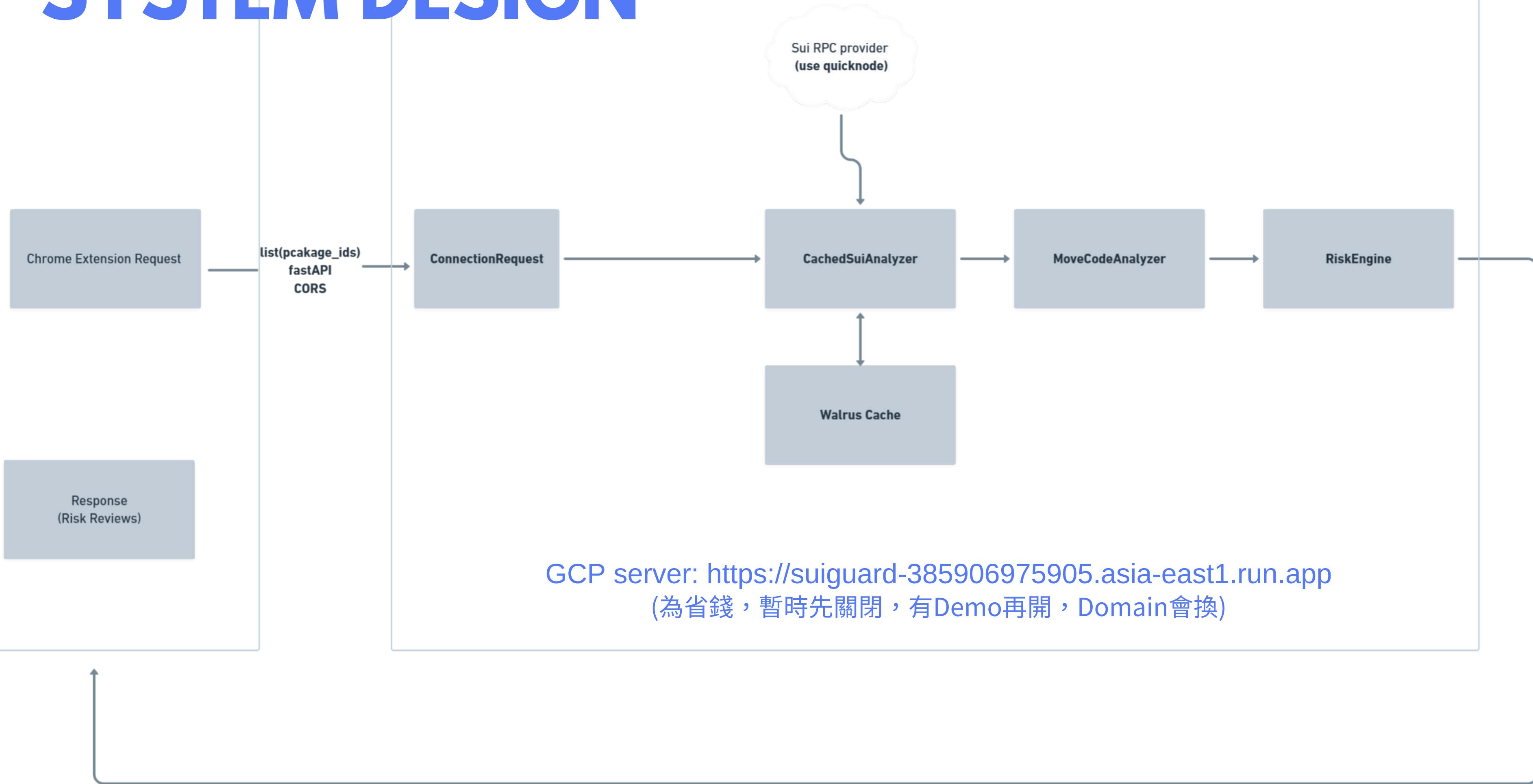
3-COLOR SECURITY LIGHT



SECURITY CERTIFICATE
(FOR BUSINESS USER)



SYSTEM DESIGN



Cloud & Chrome Extension Store

GCP server:

<https://suiguard-385906975905.asia-east1.run.app>

1. POST /api/analyze-connection
2. POST /api/analyze-versions

Rejected by Chrome Extension Store due to requesting "activeTab" permission not used in last submitted version. We use it in the new version and will resubmit.

POST https://suiguard-385906975905.asia-east1.run.app/api/analyze-connection

Params Authorization Headers (8) Body Scripts Tests Settings

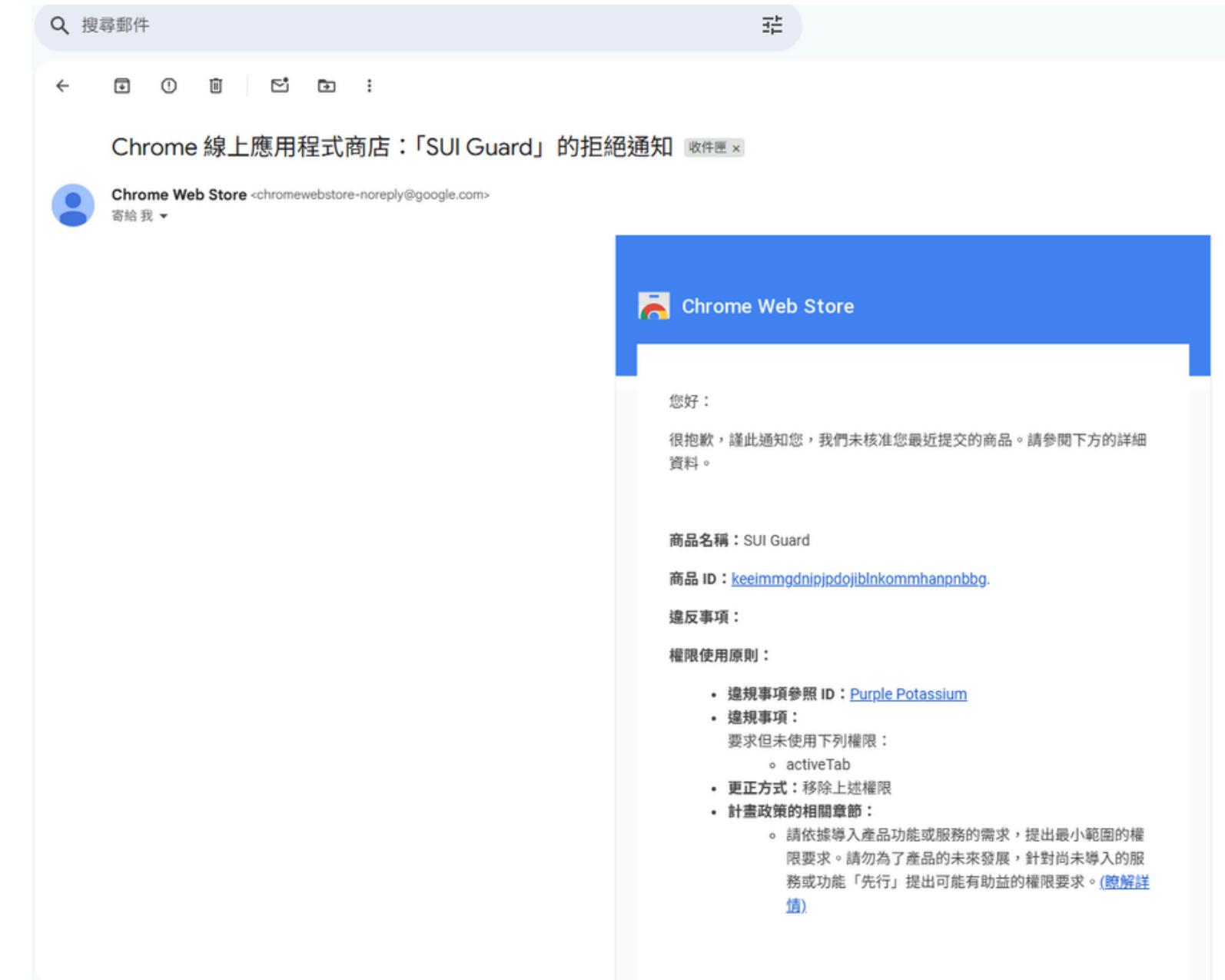
none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 {  
2   "package_ids": [  
3     "0xa998b8719ca1c0a6dc4e24a859bbb39f5477417f71885fbf2967a6510f699144"  
4   ]  
5 }
```

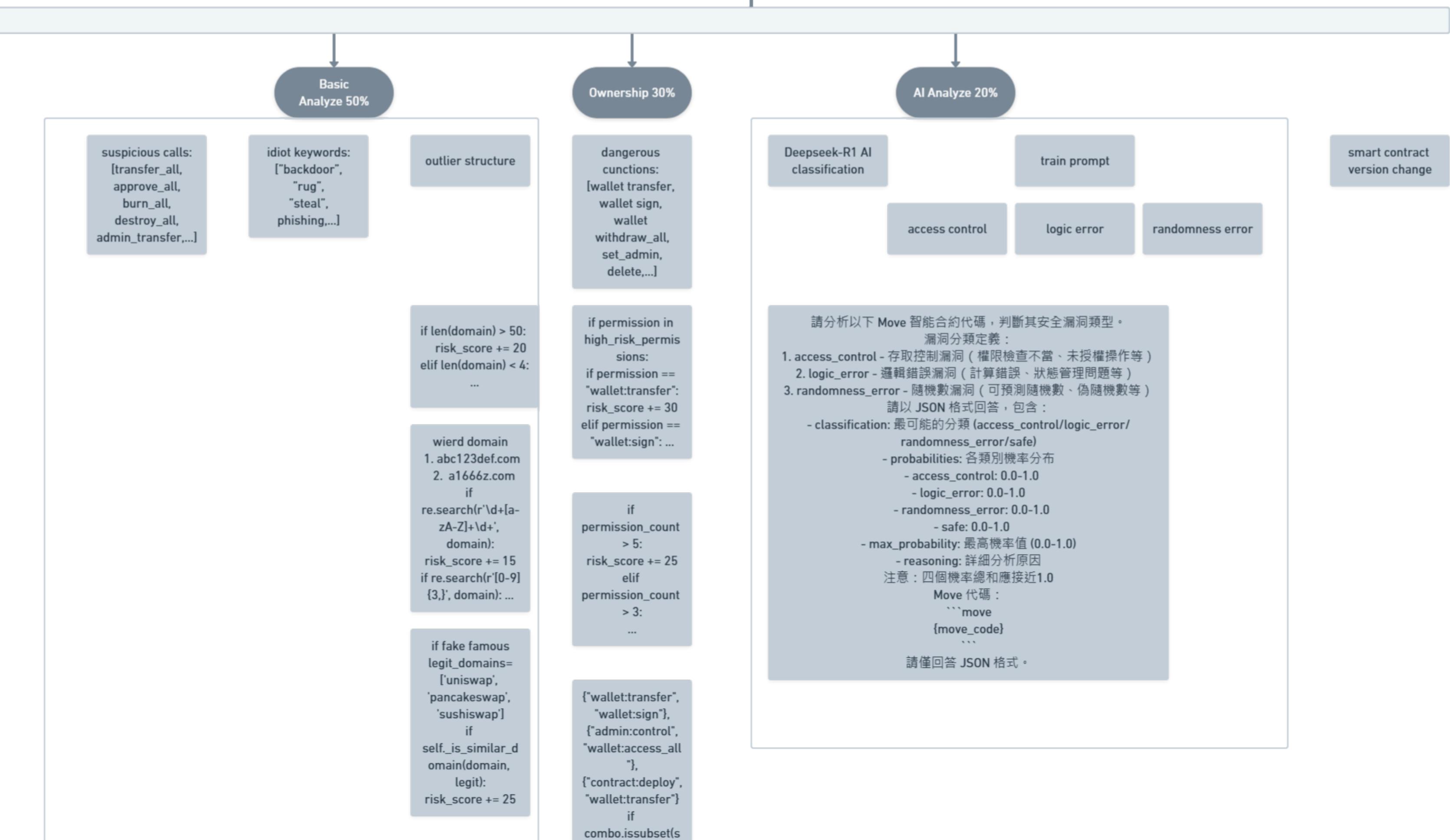
Body Cookies Headers (6) Test Results (1/1)

{ } JSON ▶ Preview ⚙ Visualize

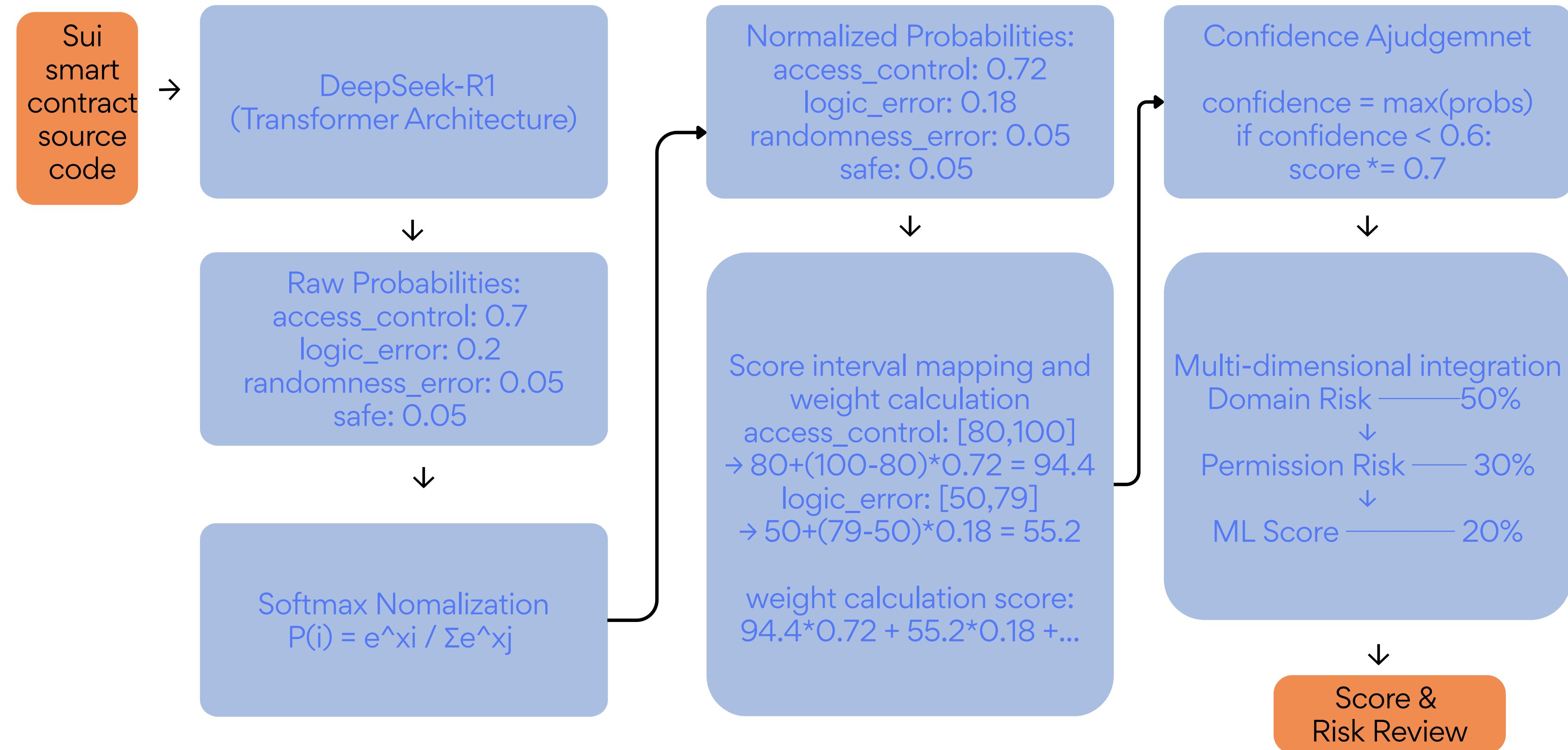
```
1 {  
2   "risk_level": "LOW",  
3   "confidence": 0.0,  
4   "reasons": [],  
5   "recommendation": "批准 - 檢測到低風險 (ML+規則引擎)",  
6   "analyzed_packages": 1,  
7   "total_packages": 1,  
8   "analysis_method": "hybrid_ml_rules",  
9   "timestamp": "2025-09-14T02:23:12.048154Z"  
10 }
```



MACHINE LEARNING METHOD(1/4)



MACHINE LEARNING METHOD(2/4)



MACHINE LEARNING METHOD(3/4)

```
[  
 {  
   "text": "module example { public fun set_admin(new_admin: address) { admin =  
 new_admin; } }",  
   "label": "access_control"  
 },  
 {  
   "text": "module bank { struct Account has store { balance: u64 } public fun withdraw(acct: &mut  
 Account, amount: u64) { acct.balance = acct.balance - amount; } }",  
   "label": "logic_error"  
 },  
 {  
   "text": "module lottery { public fun draw_winner(participants: vector<address>): address { let  
 idx = (move_to_u64(now()) % vector::length(participants)); return vector::borrow(participants,  
 idx); } }",  
   "label": "randomness_error"  
 }]
```

MACHINE LEARNING METHOD(4/4)

風險符合條件	預測類別機率分布範例	最大機率類別	風險分數範圍	置信度狀態	風險分數估算
符合第1種風險 (access_control)	{"access_control": 0.85, "logic_error": 0.10, "randomness_error": 0.05}	access_control	80 - 100	充足	$80 + (100-80)*0.85 = 97$
符合第1,2種風險 (access_control, logic_error)	{"access_control": 0.55, "logic_error": 0.40, "randomness_error": 0.05}	access_control	80 - 100	充足	$80 + (100-80)*0.55 = 91$
符合第3種風險 (randomness_error)	{"access_control": 0.10, "logic_error": 0.15, "randomness_error": 0.70}	randomness_error	20 - 49	充足	$20 + (49-20)*0.70 = 40.3$
符合第1,2,3種風險 (所有 三類均有概率)	{"access_control": 0.35, "logic_error": 0.30, "randomness_error": 0.25}	access_control	80 - 100	充足	$80 + (100-80)*0.35 = 87$

WHY SUIGUARD?

Sui Guard offers 2 plans - Free and Enterprise.

Targer Users	Pain Points	SuiGuard Solution
web3 beginners	doesn't understand any smart contract and audit report	offer badge icon, and multiple langauge warning in frontend UI
web3 users - airdrop hunters, DeFi traders	their daily work is do a lot connect, sign action, has little time to research smart contract	offer 3-color-lights, and one-click report to help them get reward points
Sui security researchers, white hats	hard to report 0-day or scam address, contracts	offer report read-time report platform
Sui project teams (protocols like Bucket, Scallop, Navi, other DeFi, Dapp)	Security issue may cause TVL down, audit is expensive and not real-time	offer cheaper and real-time solution

SUIGUARD VERSION CHECK

suivision.xyz/package/0xfa65cb2d62f4d39e60346fb7d501c12538ca2bbc646ea37ece2aec5f897814e?tab=Code

SuiVision Blockchain DeFi Coins NFTs Validators Statistics MySpace \$ 3.7815 (+1.72%) C

Package

0xfa65...814e  

Search by Coin, Account, NFT, Package, Object, Transaction, S...

Details

Publisher:  0x5ea1...9b06  

Publish Time: Jul 24, 2025 12:33:14 +UTC

Last Transaction ID: 6RVhUNRb4nkAZuttosctTWt4zBSy9UBWWaARYr22EJTg 

Version: 2

Owner: Immutable

Transaction Blocks **Code** **Statistics**

auth
blob
bls_aggregate
committee
display
encoding
epoch_parameters
event_blob

Source  Bytecode

```
1 module 0xfd88f7d7cf30afab2f82e8380d11ee8f70efb90e863d1de8616fae1bb09ea77::display {
2     struct ObjectDisplay has key {
3         id: 0x2::object::UID,
4         inner: 0x2::object_bag::ObjectBag,
5     }
6
7     struct PublisherKey has copy, drop, store {
8         dummy_field: bool,
9     }
10
11     public(friend) fun create(arg0: 0x2::package::Publisher, arg1: &mut 0x2::tx_context::TxContext) {
12         let v0 = 0x2::object_bag::new(arg1);
13         0x2::object_bag::add<0x1::type_name::TypeName, 0x2::display::Display<0xfd88f7d7cf30afab2f82e8380d11ee8f70efb90e863d1de8616fae1bb09ea77::blob>::B
14         0x2::object_bag::add<0x1::type_name::TypeName, 0x2::display::Display<0xfd88f7d7cf30afab2f82e8380d11ee8f70efb90e863d1de8616fae1bb09ea77::storage>::C>
}
```

suivision.xyz/package/0xfd88f7d7cf30afab2f82e8380d11ee8f70efb90e863d1de8616fae1bb09ea77

SuiVision Blockchain DeFi Coins NFTs Validators Statistics MySpace

Package

0xfd88...ea77  

Search by

Details

Publisher:  0x5ea1...d3ca  

Publish Time: Mar 14, 2025 10:13:58 +UTC

Last Transaction ID: 97h3LwJC5puJES4TYjtKMcktmHxqWjx9oXUVNPmbDU23 

Version: 1

Owner: Immutable

Transaction Blocks **Code** **Statistics**

Transaction Blocks

SUIGUARD CERTIFICATE

testnet.suivision.xyz / Sui Contract Package

Package

Details

Publisher: 0x876f...4b5f

Publish Time: Sep 14, 2025 03:00:06 +UTC

Last Transaction ID: 7M9iDnzpPPKV67Ewu425Jgm8UbJDwhiQd38A7UKwEHwo

Version: 1

Owner: Immutable

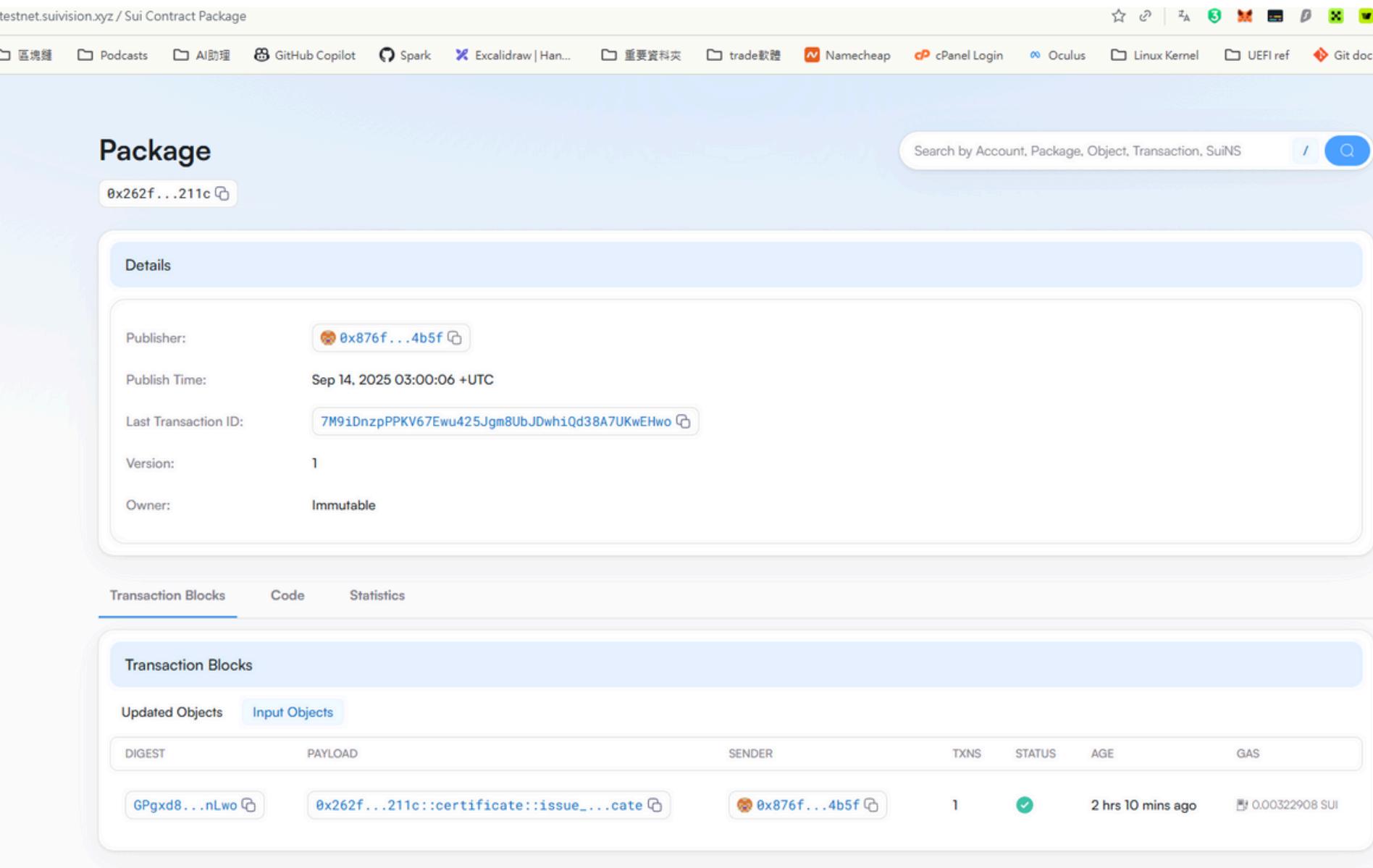
Transaction Blocks Code Statistics

Transaction Blocks

Updated Objects Input Objects

DIGEST PAYLOAD SENDER TXNS STATUS AGE GAS

GPgxd8...nLwo 0x262f...211c::certificate::issue...cate 0x876f...4b5f 1 ✓ 2 hrs 10 mins ago 0.00322908 SUI



testnet.suivision.xyz / Sui Object

SuiVision Blockchain Validators

Object

0x4bba...15f8

Details

Owner: 0x876f...4b5f

Publisher: 0x876f...4b5f

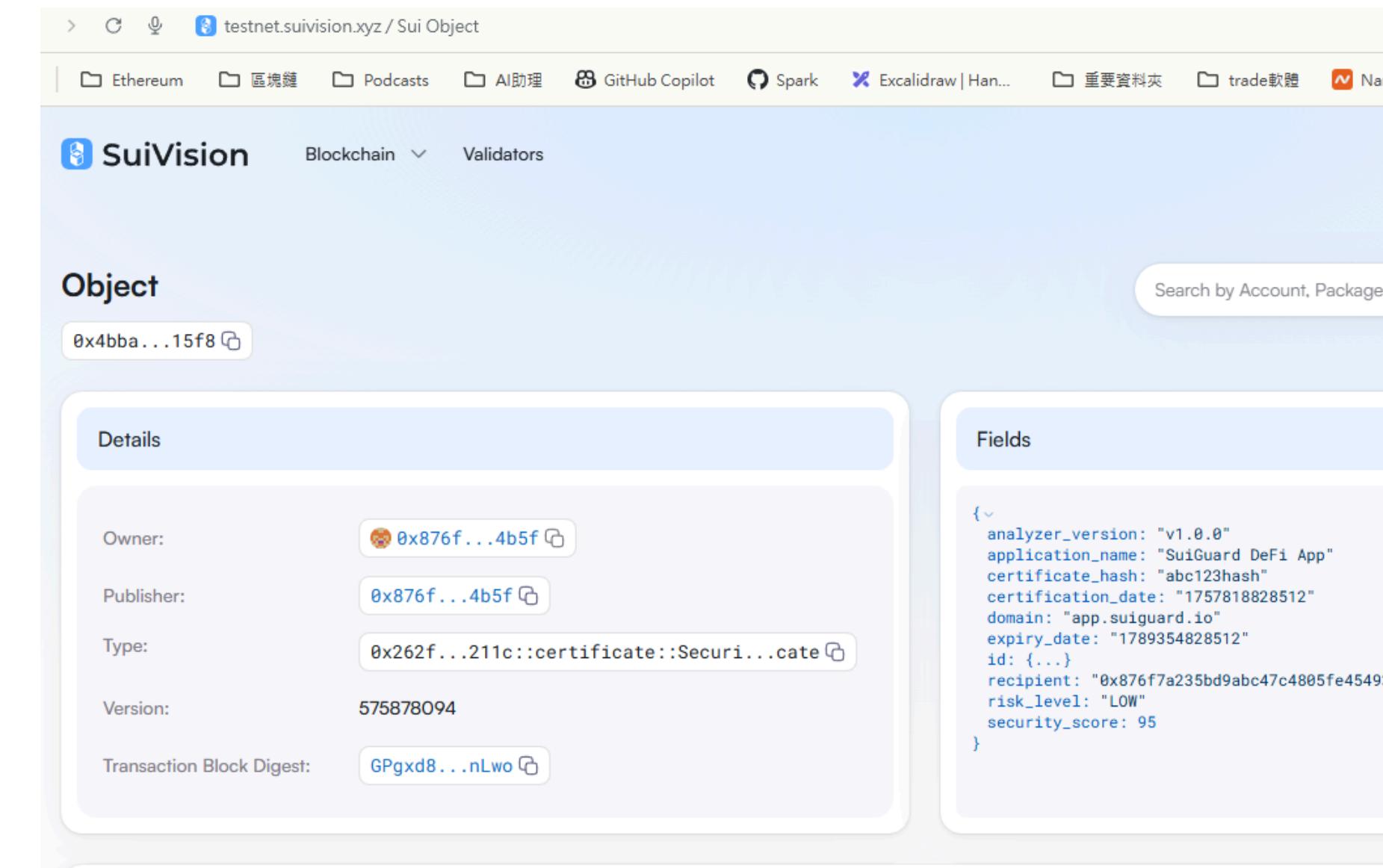
Type: 0x262f...211c::certificate::Securi...cate

Version: 575878094

Transaction Block Digest: GPgxd8...nLwo

Fields

```
{  
  analyzer_version: "v1.0.0"  
  application_name: "SuiGuard DeFi App"  
  certificate_hash: "abc123hash"  
  certification_date: "1757818828512"  
  domain: "app.suiguard.io"  
  expiry_date: "1789354828512"  
  id: {...}  
  recipient: "0x876f7a235bd9abc47c4805fe4549"  
  risk_level: "LOW"  
  security_score: 95  
}
```



CERTIFICATE CA:
**0X262FFCF89B70C1D5B486E
EDCA5D4B76B4B698160ED9
819C70AFE7F63DCE4211C**

LICENSE

license.md (MIT)

privacy.md

The screenshot shows a GitHub repository page for `k66inthesky / suiguard`. The page displays the `Privacy.md` file. The file content is as follows:

```
SUI Guard does not collect, store, or transmit any user data.

• We do not collect any personal information from users.

• No user data is ever shared or sold to any third party.

• All operations take place locally in the browser; nothing is transmitted to external servers.

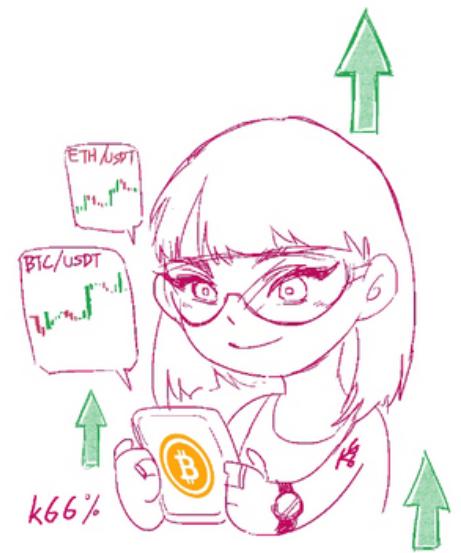
If you have any questions about privacy, please contact the developer.

Last updated: September 12, 2025
```

The GitHub interface includes navigation buttons, a sidebar with repository details, and a footer with update information.

TEAM MEMBER

k66



Backend, ML, System Design



Emily



Frontend, UI/UX, System Design



BIG THANKS

Jarek, Shawn, Maggie, Peter, Paul, VisionM

Github repo Issues(Ideas): HouseLee208, noter-wu

The screenshot shows a GitHub issue page with the URL github.com/k66inthesky/suiguard/issues/1. The issue is titled "HouseLee208 opened last week" and has the label "[idea]". The content discusses three main ideas:

- 一、【黑名單地址回報系統增強與社群協作】(屬既有功能增強)**
 - 除了基本的「雲端資料庫」和「重複回報檢查」外，可以為每個回報地址設計一個「可信度分數」，例如：根據回報人數、回報者的歷史貢獻等來計算。
 - 當使用者檢測某個地址時，如果它還不在 MysterLabs 的官方黑名單中，但已經有一定數量的 SuiGuard 使用者回報，可以顯示「此地址尚未被官方收錄，但已被 X 位使用者回報為可疑地址」。這不僅提供了額外的安全資訊，也鼓勵了社群貢獻。
- 二、【可疑/風險網站回報與告警功能】(屬延伸擴充安全性功能)**
 - 在「檢查/回報可疑地址」的當下，自動記錄當前網頁網址，能為「可疑網站候選清單」提供一個高價值的、基於使用者行為的數據來源。
 - 建立關聯性 (Contextual Linking)，產出「待審核清單」：
前述機制能建立「可疑地址」與「使用該地址的網站」之間的直接關聯。提供某種證據鏈。
當一個網址被多個使用者從不同的回報中記錄下來時，就可以自動提升其風險評級，進入「待審核清單 (Pending Review List)」。並觸發後續的審核流程。
- 三、【從Chrome Extension 到「Web3 威脅情報與教育中心」】(長期服務規劃)**
 - 建立視覺化威脅情報儀表板，例如：
 - 實時威脅地圖：顯示全球使用者回報的可疑地址與網站分佈，幫助使用者對當前的威脅態勢一目了然。
 - 熱門詐騙清單：根據回報次數和風險等級，列出當前最常被回報的可疑網站或惡意地址，提供即時參考。

At the bottom right, there is a note in Chinese: "的活躍程度，這有助於社群了解趨勢" (The level of activity, which helps the community understand trends).

HouseLee208 opened last week

【idea】

一、【黑名單地址回報系統增強與社群協作】(屬既有功能增強)

- 1.除了基本的「雲端資料庫」和「重複回報檢查」外，可以為每個回報地址設計一個「可信度分數」，
例如：根據回報人數、回報者的歷史貢獻等來計算。
- 2.當使用者檢測某個地址時，如果它還不在 MysterLabs 的官方黑名單中，
但已經有一定數量的 SuiGuard 使用者回報，可以顯示
「此地址尚未被官方收錄，但已被 X 位使用者回報為可疑地址」。
這不僅提供了額外的安全資訊，也鼓勵了社群貢獻。

二、【可疑/風險網站回報與告警功能】(屬延伸擴充安全性功能)

- 1.在「檢查/回報可疑地址」的當下，自動記錄當前網頁網址，
能為「可疑網站候選清單」提供一個高價值的、基於使用者行為的數據來源。
- 2.建立關聯性 (Contextual Linking)，產出「待審核清單」：
前述機制能建立「可疑地址」與「使用該地址的網站」之間的直接關聯。提供某種證據鏈。
當一個網址被多個使用者從不同的回報中記錄下來時，就可以自動提升其風險評級，進入「待審核清單 (Pending Review List)」。

JOIN US!



Welcome to open Issues and Pull Requests!



REFERENCE

<https://suivision.xyz/txblock/HMMicxQWn43rnNswi4gNHanUaeWW5ijqM5bHLca67D9?tab=Changes>

<https://www.securityalliance.org/news/2025-09-npm-supply-chain>

<https://www.pcrisk.com/removal-guides/32322-sui-airdrop-scam>

<https://arxiv.org/html/2508.17964v1>

<https://blog.sui.io/sui-guardians-community-driven-defense/>

<https://jdstaerk.substack.com/p/we-just-found-malicious-code-in-the>