PITCH DECK

MONITORING & DEFI RISK DETECTION SYSTEM

on Sui Blockchain

Thuyết trình *Hoàng Đức Bách*
Giảng viên *Lê Khánh Trình*

Đại học Công nghệ
Đại học Quốc gia Hà Nội

5 Dec, 2025

MỤC LỤC

1. GIỚI THIỆU

Dự án này sẽ trình bày về Hệ thống Giám sát và Phát hiện rủi ro Defi trên hệ sinh thái Sui Blockchain (gọi tắt là MDRDS).

Hệ thống sử dụng ELK Stack (1 trong những bộ công cụ nguồn mở cho việc thu thập, tìm kiếm, phân tích và trực quan hóa dữ liệu một cách an toàn) kế hợp sâu với Sui Infrastructure để triển khai việc thu thập, cũng như phân tích với các transaction của protocol sử dụng Move Contract (bằng việc khai thác sức mạnh của Object-Centric Model cho việc phân tích assets và movement của assets thông qua TX-DAG và Event-based có cấu trúc trên Sui)

Hệ thống MDRDS sẽ cung cấp:

Near Realtime Transaction Monitoring

Theo dõi và phân tích trực quan transaction với độ trễ thấp (<5s) trên *Kibana* (qua *Elastic*) và near realtime (1-2s) cho detect ở Custom Indexer (qua *Postgres*)

Multi-dimensional Risk Detection

Đưa ra hướng tiếp cận mới cho phân tích các vector attacks khác nhau

Tracing & Behavioral Analysis

Cung cấp khả năng truy vết và phân tích hành vi của người dùng dựa trên dữ liệu lịch sử (historical data) để phát hiện risk phức tạp bằng Elastic Query

1. GIỚI THIỆU

Hệ thống được thiết kế cho các DeFi Protocol vận hành trên blockchain Sui để:

HEALTH

Theo dõi tình sức khoẻ protocol và phát hiện các bất thường theo thời gian thực

RISK DETECTION

Nhận cảnh báo sớm về các cuộc tấn công tiềm ẩn trước khi xảy ra tổn thất đáng kể

ANALYSIS

Phân tích các mô hình lịch sử để cải thiện tình hình an ninh

RESPONSE

Thực hiện các hành động phòng thủ tự động (tạm dừng hợp đồng, điều chỉnh thông số, cảnh báo các bên liên quan)

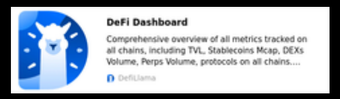
KIM CHỈ NAM

“Xây dựng một hạ tầng thu thập và phân tích giao dịch mạnh mẽ, mở rộng lâu dài trên Elastic Stack; đồng thời nghiên cứu sâu các rủi ro DeFi hiện nay để phát triển các thuật toán phát hiện bất thường và cơ chế phòng vệ giúp các protocol vận hành an toàn, ổn định và bền vững.”

2. BỐI CẢNH & VẤN ĐỀ

Global DeFi TVL

$120-150 billion (2024-2025)



Sui DeFI TVL

$951 million (2025)

Crypto Hack Losses

$1,668,990,884 (Q1- 2025) *≈ 70% 2024*

DeFi Attack Report

83,3% Flash Loan attacks (2024)

32,1% Market Manipulation attacks (2021)

15% Rug pull / Sccam (2024)

5,6% Governance attacks (2024)

55,6% total losses on Compromise Wallet (2025)

Dựa trên các thống kê từ *DefiLlama*, *CertiK* và *Halborn*, có thể thấy DeFi tiếp tục mở rộng mạnh mẽ nhưng đi kèm là sự gia tăng cả về số lượng lẫn độ tinh vi của các cuộc tấn công. Trong nhóm tấn công on-chain, Direct Contract Exploits luôn chiếm tỷ trọng lớn, đặc biệt là Price Manipulation và Flash Loan–những hình thức rất khó phân định ranh giới giữa giao dịch hợp pháp và tấn công.

Song song đó, dữ liệu từ *Halborn* cho thấy một xu hướng đáng lo ngại: Compromised Accounts (tài khoản bị chiếm quyền kiểm soát) hiện chiếm >50% số vụ tấn công và ~47% tổng giá trị thiệt hại. Đây là nhóm tấn công cực khó phát hiện bằng cách phân tích giao dịch đơn lẻ, vì hacker ký giao dịch bằng private key hợp lệ

Các attacks tiếp tục gia tăng với nhiều biến thể mới, cho thấy DeFi cần một hệ thống quan sát và cảnh báo sớm mạnh mẽ hơn để bảo vệ toàn bộ hệ sinh thái.

2. BỐI CẢNH & VẤN ĐỀ

Evolving DeFi Threats

Các cuộc tấn công DeFi vẫn đang phát triển về quy mô và ngày càng tinh vi với nhiều biến thể phức tạp, khai thác lỗ hổng trên nhiều protocol.

Attack Vector Coverage

Công cụ bảo mật hiện nay chủ yếu giám sát ở mức từng protocol, dẫn đến khoảng trống trong việc phát hiện các vector tấn công phức tạp liên quan đến nhiều giao dịch và hành vi lịch sử, điển hình như dòng tiền phối hợp hay rửa tiền.

Lack of Comprehensive Threat Detection

DeFi trên Sui đang phát triển mạnh, nhưng hiện thiếu một hệ thống phòng thủ liên tục, giám sát và phản ứng với mối đe dọa toàn diện trên tất cả các protocol.

2. BỐI CẢNH & VẤN ĐỀ

Phân loại các cuộc tấn công *(Halborn)*

Off-chain attacks

Các vụ hack mà nguyên nhân chính xảy ra ngoài blockchain (ví dụ: lộ private key, hack server, chiếm tài khoản)

Compromised Account

On-chain attacks

Các vụ hack mà lỗ hổng nằm ngay trên blockchain

Market Price Manipulation

Direct contract exploitation

Governance Attacks

Both type of attacks

Team rút sạch thanh khoản hoặc tiền người dùng rồi biến mất — gồm cả Ponzi, nội gián, CEO rút quỹ.

- Nếu dùng backdoor hoặc quyền on-chain → on-chain attack.
- Nếu lừa ngoài blockchain → off-chain attack.

3. CÁC GIẢI PHÁP

1. Dual-Layer Detection Architecture

Hệ thống kết hợp **giám sát giao dịch near realtime** với **bộ công cụ phân tích tổng hợp hành vi dựa trên lịch sử qua Elastic**, mang lại khả năng phát hiện mối đe dọa toàn diện và nhận diện hiệu quả các vector tấn công.

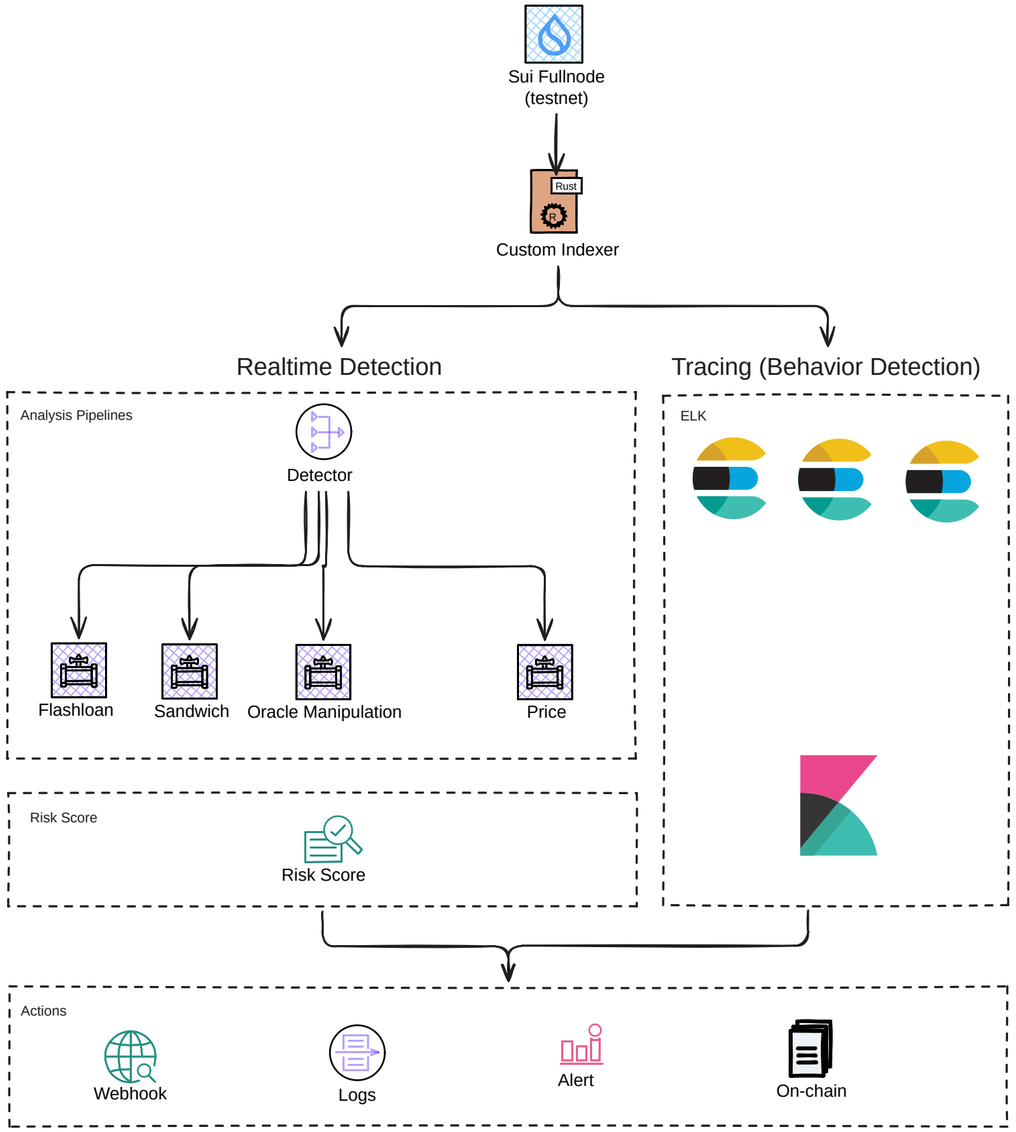
2. Multi-Signal Graduated Risk Scoring

Hệ thống sử dụng nhiều tín hiệu (signal) để đánh giá rủi ro một cách đa chiều, cung cấp phân loại các rủi ro chi tiết và cho phép phản ứng tỉ lệ thuận với mức nguy cơ.

3. Enterprise-Scale Behavioral Analysis

Phân tích hành vi lịch sử có quy mô, tổng hợp dữ liệu **on-chain** và **off-chain**, phát hiện các tấn công phối hợp và rủi ro bất thường.
Trực quan hóa rủi ro theo thời gian thực, hỗ trợ truy vết nguồn gốc, dự đoán tấn công và đưa ra các phép phản ứng

4. KIẾN TRÚC


Sui Fullnode
(testnet)
Rust
Custom Indexer
Realtime Detection
Tracing (Behavior Detection)
Analysis Pipelines
Detector
Flashloan
Sandwich
Oracle Manipulation
Price
ELK
Risk Score
Risk Score
Actions
Webhook
Logs
Alert
On-chain

4. KIẾN TRÚC

Multi-Signal

Sử dụng đa-tín-hiệu (multi-signal) dùng để phát hiện sớm các tấn công DeFi có độ phức tạp cao

Oracle Manipulation Analyzer
Độ lệch giá oracle, swap tác động lớn, abnormal HF, ước tính tổn thất protocol.

Flash Loan Analyzer
Nhận diện vòng lặp arbitrage, multi-pool, swap chain, price impact

Sandwich Analyzer
Stateful, phát hiện front-run → victim → back-run theo checkpoint

Price Analyzer
TWAP deviation, trade-to-liquidity ratio và price impact.

4. KIẾN TRÚC

Elastic Stack

ELK đóng vai trò trung tâm lưu trữ và phân tích dữ liệu on-chain. Cung cấp một công cụ quan sát tổng thể cho protocol

Ingestion
Thu thập & index toàn bộ giao dịch, sự kiện, logs theo thời gian với độ trễ thấp.

Query (using DSL)
Truy vấn nhanh các pattern bất thường: wash trading, price manipulation, money laudring...

Aggregation
Phân tích thống kê (extended stats) để đo biến động, price impact, volume spikes.

Visualization
Kết nối dashboard (Kibana) để giám sát và cảnh báo trực quan, thông qua các native features mạnh như Lens, TSVB và custom chart giúp phân tích pattern tấn công rõ ràng và theo thời gian thực.

Actions
Kích hoạt alert kèm các actions tự động khi có hành vi bất thường vượt threshold.

5. DEMO

Trình bày demo tổng quan hệ thống MDRDS, bao gồm vận hành hệ thống và mô phỏng các cuộc tấn công thực tế để kiểm thử.

5. DEMO

Part 1: Giới thiệu tổng quan

Đi qua nhanh kiến trúc hệ thống, các ý tưởng và cải tiến tương lai

Part 2: Giả lập các attacks và test Realtime Detection

Giới thiệu nhanh về protocol sử dụng cùng các kịch bản, input và expected output; chạy tuần tự và kiểm tra kết quả.

Part 3. Giả lập giao dịch và test Tracing

Giới thiệu về ELK, mục đích và hướng tiếp cận như đã trình bày với ELK. Input một loạt các test transactions (generation). Các kịch bản query và hướng tiếp cận dài hạn

Thank **You**

www.reallygreatsite.com - hello@reallygreatsite.com