CyStack

DATA SHEET

On-chain Monitoring Powered by SafeChain

Real-time protection for the blockchain network

Overview

On-chain security monitoring is the process of monitoring the activity on a blockchain network to detect and respond to any potential security threats or breaches. This can include monitoring for suspicious transactions, unusual patterns of activity, or attempts to exploit vulnerabilities in the network. The goal of on-chain security monitoring is to detect and respond to potential threats as quickly as possible to protect the integrity of the blockchain and the assets stored on it. It is important for several reasons: it is a decentralized network and there is no central authority responsible for ensuring the security of the network, blockchain networks are transparent and immutable, the increase of the value and significance of blockchain technology has grown, so has the interest of hackers and bad actors looking to exploit vulnerabilities in the system and the use of smart contracts on blockchain networks has increased the risk of security breaches.

Customer Benefits

- Real-time threat detection
- Real-time significant price drop detection
- Automated response to potential breaches
- Multi-chain support
- Scammer detection

How CyStack Helps

CyStack's on-chain monitoring solution, SafeChain, is a scalable security solution that leverages automated technologies to monitor activities on the blockchain which focuses on:

- **Real-time threat detection**: SafeChain uses advanced algorithms and machine learning techniques to analyze blockchain activity in real time, providing customers with near-instant alerts of any potential security threats or breaches.
- **Automated response**: SafeChain can be configured to automatically respond to security threats, such as rolling back transactions or freezing assets, minimizing the impact of a security breach.
- **Customized monitoring**: SafeChain can be customized to meet the specific needs of a customer's environment, allowing for tailored monitoring and response to potential threats.
- **Compliance**: SafeChain can help customers comply with regulations and standards by providing a comprehensive view of all activities on their blockchain network, making it easier to identify and report any suspicious activity.
- **Comprehensive reporting**: SafeChain provides detailed reporting on all blockchain activity, including historical data, making it easy for customers to identify patterns or anomalies that may indicate a security threat.
- **Multi-chain support**: SafeChain can monitor multiple blockchain networks, providing customers with a unified view of their blockchain security posture.

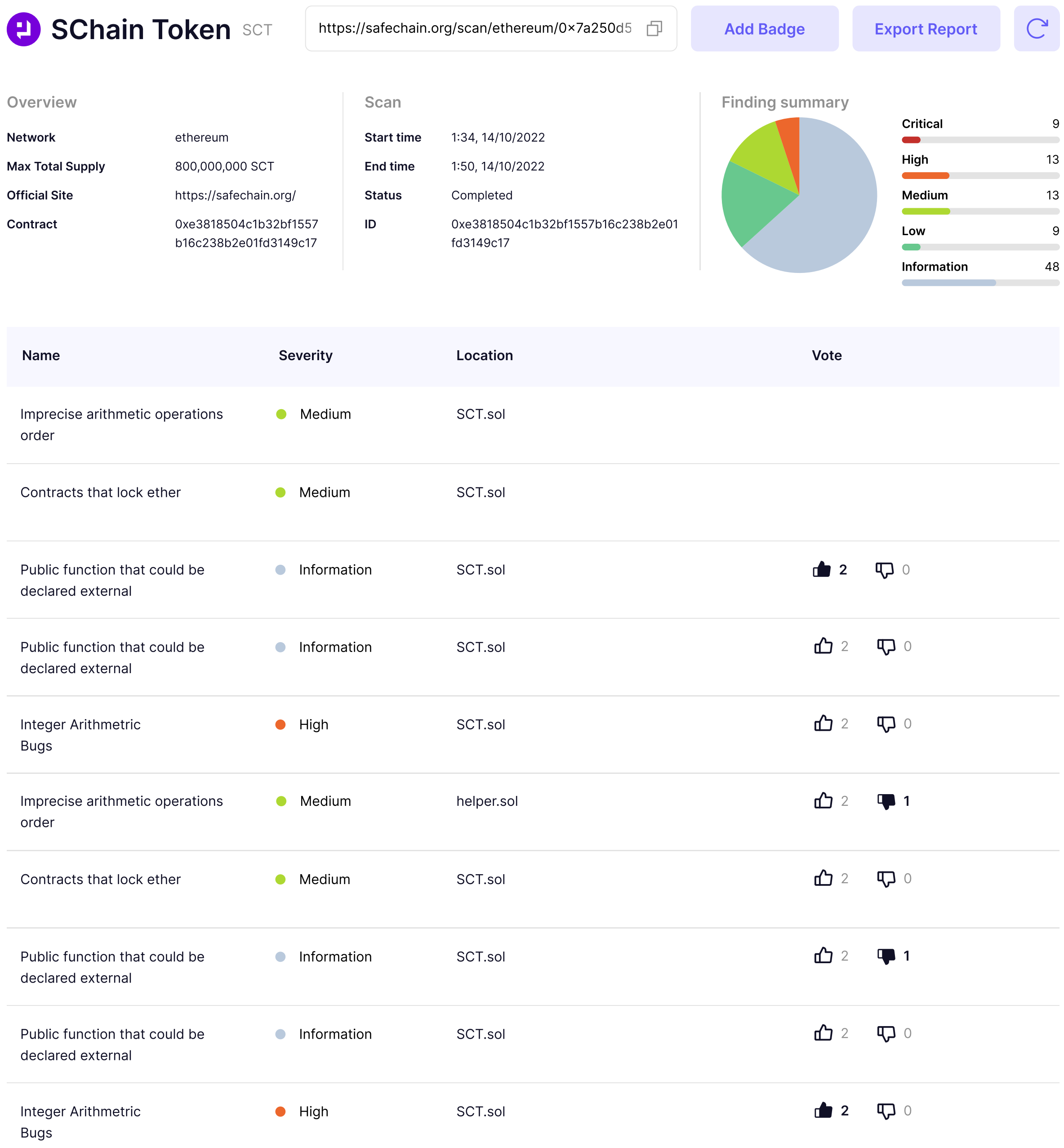
Automated Vulnerability Scanning

SafeChain is a comprehensive on-chain monitoring solution that includes an automated vulnerability scanner specifically designed for blockchain networks. The scanner is capable of downloading smart contracts from various testnets and mainnets, including Ethereum, Ropsten, Kovan, Rinkeby, Goerli, BSC, Testnet BSC, Arbi, Testnet Arbi, Polygon, Avax, Testnet Avax, and FTM.

Once downloaded, the scanner analyzes the smart contracts for common vulnerabilities, such as those related to the Solidity programming language or the underlying blockchain platform. The scanner checks for known vulnerabilities and exploitable code patterns, as well as tests the smart contract's logic and functionality. This helps to identify any potential attack vectors that could be used to compromise the integrity of the network and provide actionable insights on how to remediate them.

Key Features

- Automated smart contract vulnerability scanning
- Price drop alerting
- Scammer detection
- API integration



Overview

Network	ethereum
Max Total Supply	800,000,000 SCT
Official Site	https://safechain.org/
Contract	0xe3818504c1b32bf1557b16c238b2e01fd3149c17

Scan

Start time	1:34, 14/10/2022
End time	1:50, 14/10/2022
Status	Completed
ID	0xe3818504c1b32bf1557b16c238b2e01fd3149c17

Finding summary

Critical	9
High	13
Medium	13
Low	9
Information	48

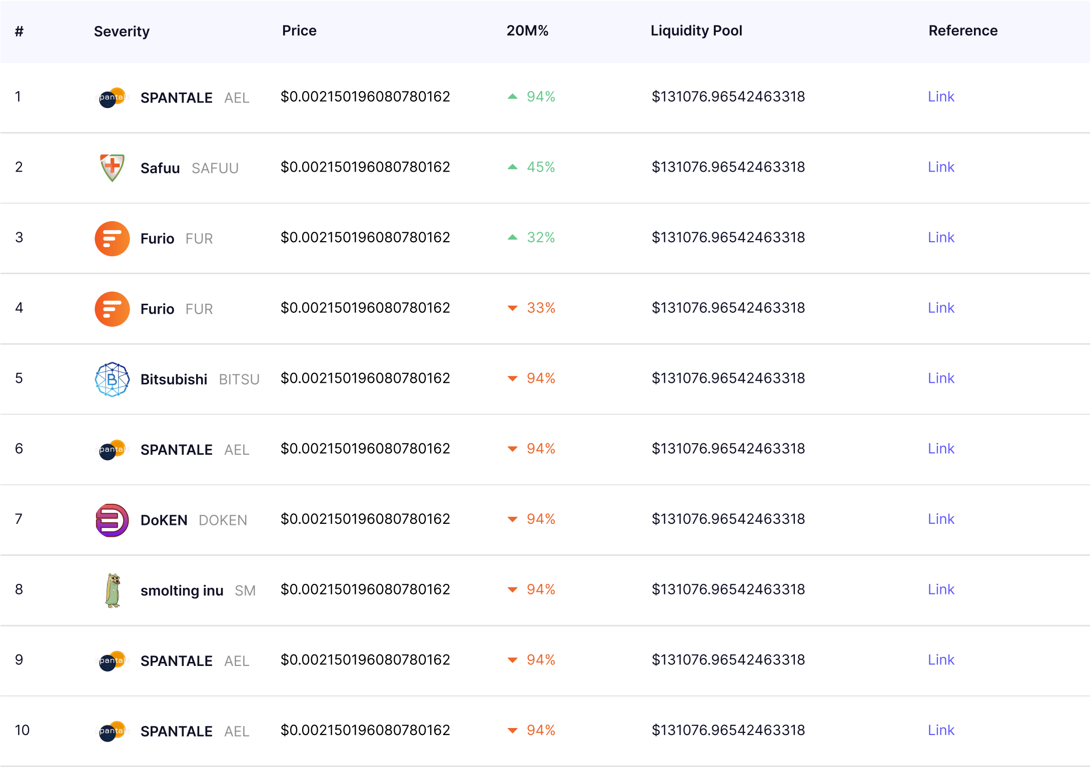
Name	Severity	Location	Vote
Imprecise arithmetic operations order	● Medium	SCT.sol	
Contracts that lock ether	● Medium	SCT.sol	
Public function that could be declared external	● Information	SCT.sol	👍 2 👎 0
Public function that could be declared external	● Information	SCT.sol	👍 2 👎 0
Integer Arithmetric Bugs	● High	SCT.sol	👍 2 👎 0
Imprecise arithmetic operations order	● Medium	helper.sol	👍 2 👎 1
Contracts that lock ether	● Medium	SCT.sol	👍 2 👎 0
Public function that could be declared external	● Information	SCT.sol	👍 2 👎 1
Public function that could be declared external	● Information	SCT.sol	👍 2 👎 0
Integer Arithmetric Bugs	● High	SCT.sol	👍 2 👎 0

Our scanner will test the following types of vulnerabilities:

1. **Reentrancy**: This type of vulnerability occurs when a smart contract allows an attacker to repeatedly call it and extract its value multiple times.
2. **Unchecked call return value**: This type of vulnerability occurs when a smart contract does not properly check the return value of a call to another contract, which can lead to the execution of malicious code.
3. **Unchecked user input**: This type of vulnerability occurs when a smart contract does not properly validate user input, which can lead to the execution of malicious code or the manipulation of data.
4. **Unchecked math operations**: This type of vulnerability occurs when a smart contract uses math operations that can overflow or underflow, leading to unintended results.
5. **Unchecked external calls**: This type of vulnerability occurs when a smart contract calls an external contract without properly checking the return value, which can lead to the execution of malicious code or the manipulation of data.
6. **Integer overflow and underflow**: This type of vulnerability occurs when a smart contract does not properly handle large numbers, which can lead to unintended results.
7. **Unsecured data storage**: This type of vulnerability occurs when a smart contract stores sensitive data in an unsecured manner, which can lead to data breaches.
8. **Timestamp dependence**: This type of vulnerability occurs when a smart contract is dependent on the timestamp provided by the blockchain network, which can be manipulated by an attacker.
9. **Unsecured randomness**: This type of vulnerability occurs when a smart contract uses an insecure random number generator, which can be predicted by an attacker.
10. **Access control**: This type of vulnerability occurs when a smart contract does not properly implement access control, which can allow unauthorized parties to access or manipulate data.

Cryptocurrency Price Drop

The price of cryptocurrency is known to be highly volatile, with prices fluctuating rapidly and sometimes experiencing significant drops. This volatility can make it difficult for investors to make informed decisions and can increase the risk of financial losses.



#	Severity	Price	20M%	Liquidity Pool	Reference
1	SPANTALE AEL	$0.002150196080780162	▲ 94%	$131076.96542463318	Link
2	Safuu SAFUU	$0.002150196080780162	▲ 45%	$131076.96542463318	Link
3	Furio FUR	$0.002150196080780162	▲ 32%	$131076.96542463318	Link
4	Furio FUR	$0.002150196080780162	▼ 33%	$131076.96542463318	Link
5	Bitsubishi BITSU	$0.002150196080780162	▼ 94%	$131076.96542463318	Link
6	SPANTALE AEL	$0.002150196080780162	▼ 94%	$131076.96542463318	Link
7	DoKEN DOKEN	$0.002150196080780162	▼ 94%	$131076.96542463318	Link
8	smolting inu SM	$0.002150196080780162	▼ 94%	$131076.96542463318	Link
9	SPANTALE AEL	$0.002150196080780162	▼ 94%	$131076.96542463318	Link
10	SPANTALE AEL	$0.002150196080780162	▼ 94%	$131076.96542463318	Link

SafeChain includes a real-time price tracking feature that allows users to know if the value of their assets experiences a significant drop in near real-time. This can help users to detect price drops and respond quickly by taking appropriate action such as selling the asset or holding on to it until the price recovers.

It's really important for both crypto investors and blockchain companies because of:

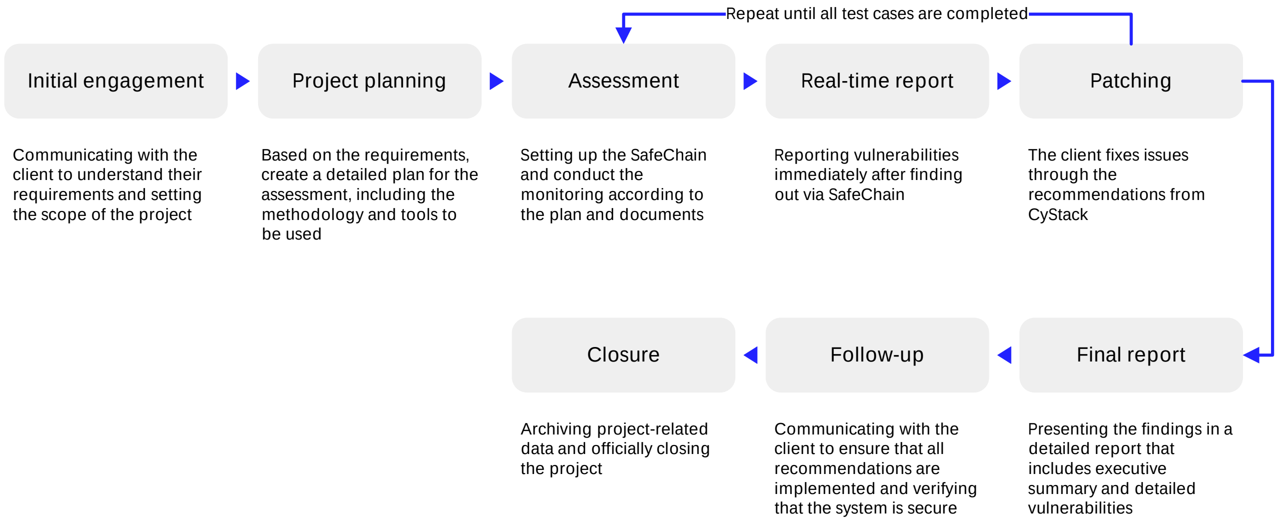
- **Detecting market manipulation**: Monitoring pricing drops on-chain can help detect instances of market manipulation, such as when a group of individuals or entities artificially lower the price of a cryptocurrency in order to profit from short-selling.
- **Identifying security breaches**: A sudden and significant drop in price could be an indication of a security breach, such as a hack or a loss of private keys. By using this feature, it's possible to detect such incidents and take appropriate action to minimize the damage.
- **Protecting assets**: Users can identify when the value of a particular asset is decreasing and take action to protect their investments, such as selling the asset or holding on to it until the price recovers.

And More...

SafeChain offers Scam Watch, which is a specialized tool designed to detect scammers on crypto exchanges. The Scam Watch uses advanced algorithms to analyze blockchain activity in real time, providing near-instant alerts of any potential scams or fraudulent activities. It is also designed to allow users to report scams they have witnessed or encountered. Our moderators will double-check these reports to blacklist scammers. Scam Watch is being made available as API, making it easy for other developers and companies to integrate it into their own applications, allowing everyone to use it. This can help to improve the overall security of the crypto space by making it more difficult for scammers to operate.

SafeChain also plans to monitor anomalies happening on the blockchain, this can help detect potential security threats, market manipulation, and other suspicious activities. This can provide an early warning system for potential issues, allowing users to take appropriate action to protect their assets.

Flow To Work With Clients



Repeat until all test cases are completed

Initial engagement

Communicating with the client to understand their requirements and setting the scope of the project

Project planning

Based on the requirements, create a detailed plan for the assessment, including the methodology and tools to be used

Assessment

Setting up the SafeChain and conduct the monitoring according to the plan and documents

Real-time report

Reporting vulnerabilities immediately after finding out via SafeChain

Patching

The client fixes issues through the recommendations from CyStack

Final report

Presenting the findings in a detailed report that includes executive summary and detailed vulnerabilities

Follow-up

Communicating with the client to ensure that all recommendations are implemented and verifying that the system is secure

Closure

Archiving project-related data and officially closing the project

About CyStack

CyStack is an innovative company in the field of cybersecurity in Vietnam. We are a pioneer in building next gen security products for businesses and individuals. Our solutions focus on data protection, cyber attack prevention, and security risk management.

☎

For more information, please call **(+84) 247 109 9656** or send an email to **contact@cystack.net** to speak to CyStack security specialist.
cystack.net

CyStack