EXTRACTOR
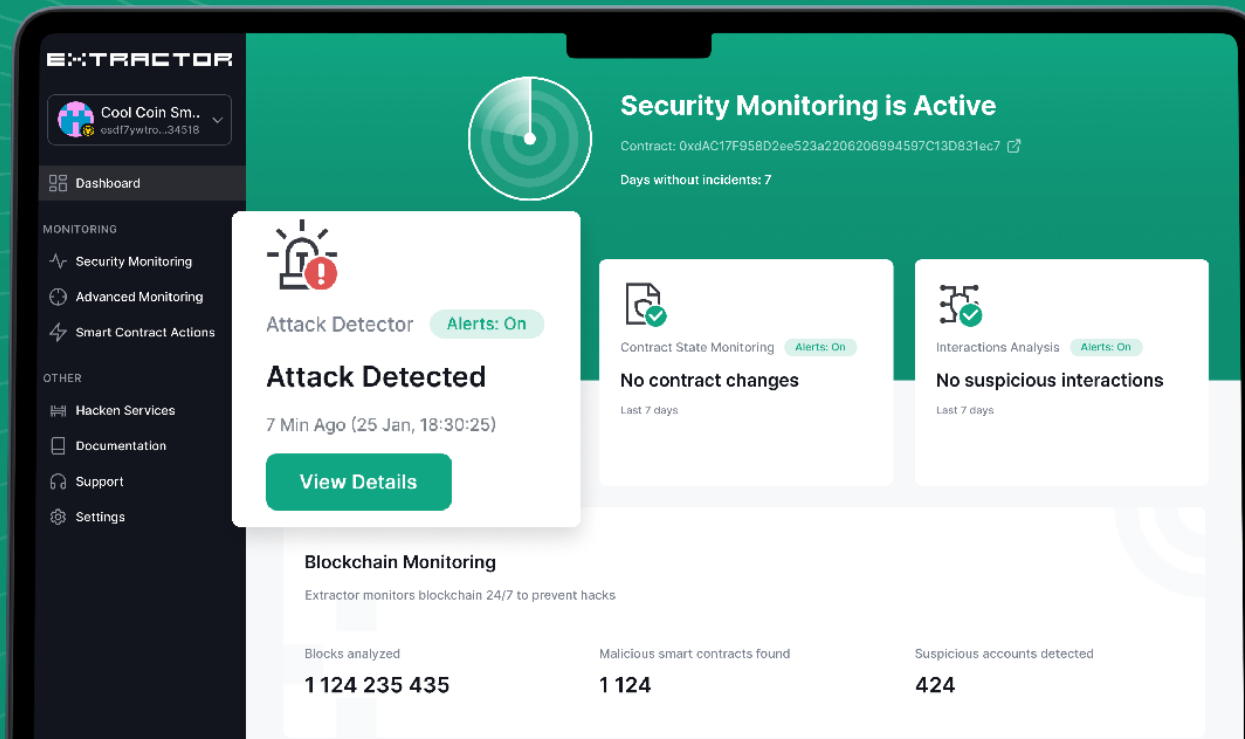
Post-deployment Security Solution for Attacks Detection and Prevention
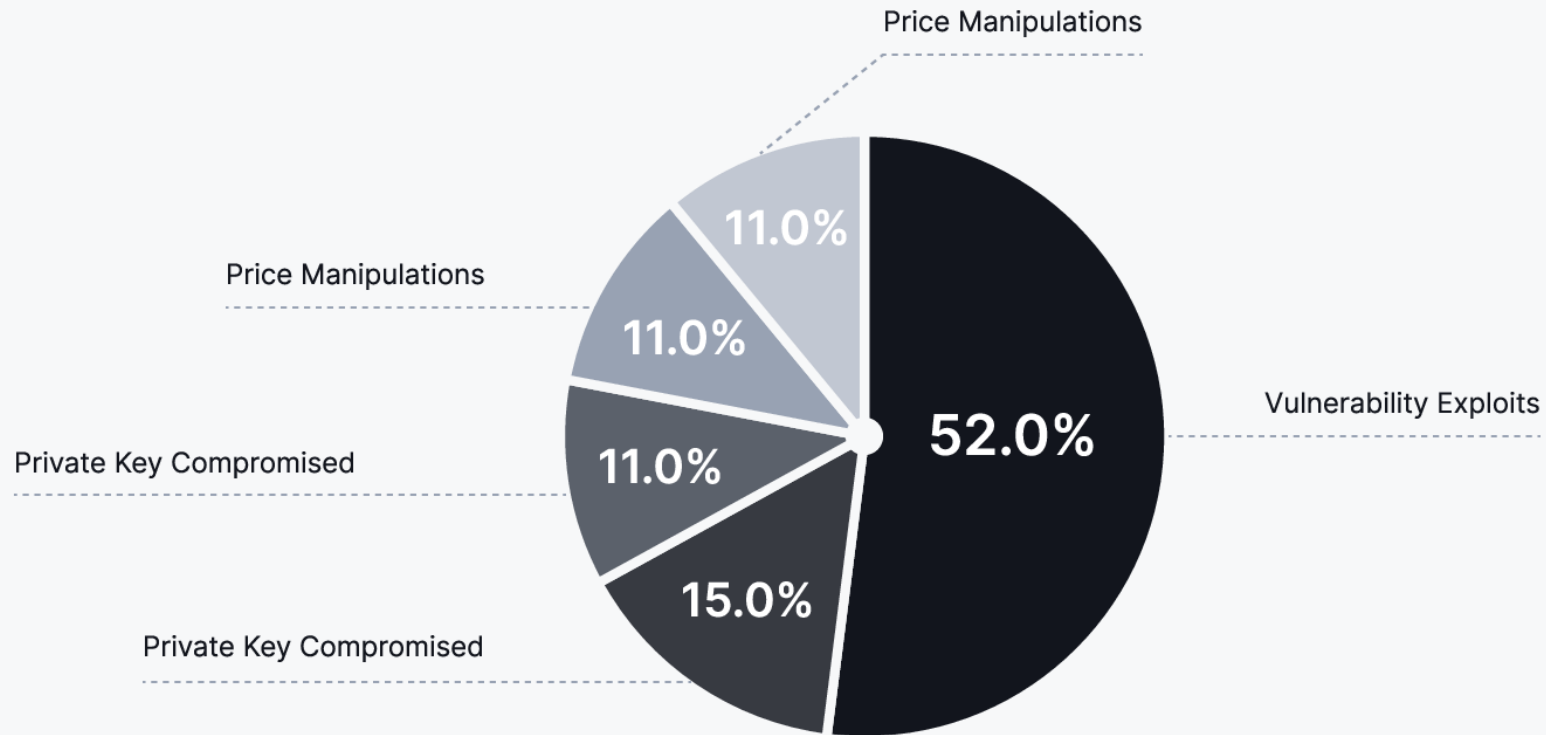
Web3 security practices on code development, testing, and deployment are **not enough** to provide comprehensive protection against hacks.

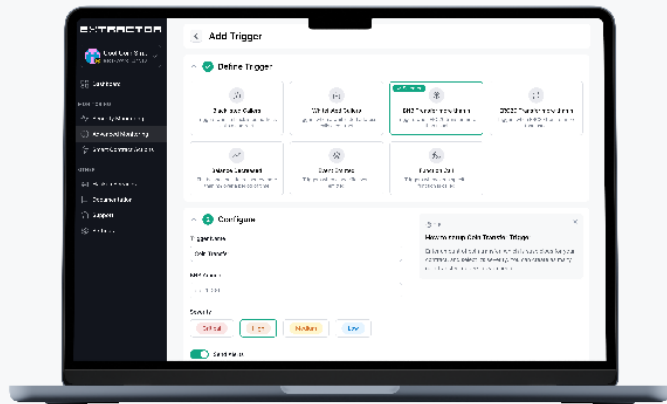$1 Billion was spent securing smart contracts in 2022

$4 Billion was hacked last year

Price Manipulations

Price Manipulations

Private Key Compromised

Private Key Compromised

Vulnerability Exploits

11.0%

11.0%

11.0%

52.0%

15.0%

Post Deployment security approach, which includes real-time monitoring, detection, and protection mechanisms, become essential.


EXTRACTOR

Extractor - adopts a holistic security strategy that combines pre-deployment practices with ongoing monitoring and crucial response mechanisms to fortify Web3 ecosystem against the ever-evolving threat landscape.

Our mission - is to make Web3 a safer place for all projects by offering advanced security solutions.

Extractor provides post-deployment security solutions covering smart contracts, transaction monitoring, and security tools.
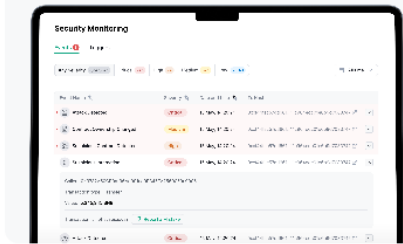
Transactions Monitoring (block-level transaction and contract call detection) with user-defined triggers
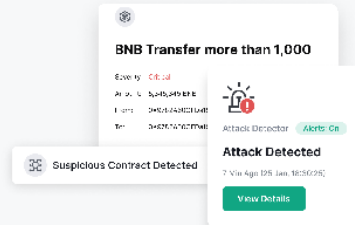
Attack Detection (multi-step complex scenario attack vectors detection)

Alerts and Actions on Triggers

Blockchains Integration (Ethereum, Arbitrum, BSC, ICP, VeChain, ...)

How does it work?

Security Monitoring of Smart Contracts

Detecting Attacks and Hacks by monitoring and defining suspicious accounts and smart contracts on chain.

Advanced Monitoring of Smart Contracts

Setup additional triggers depending on projects types that are detecting suspicious events across the Smart Contract

Hacks Prevention Mechanisms

From no code to full integration mechanisms that allow automated response to incidents to mitigate risks or completely prevent exploit
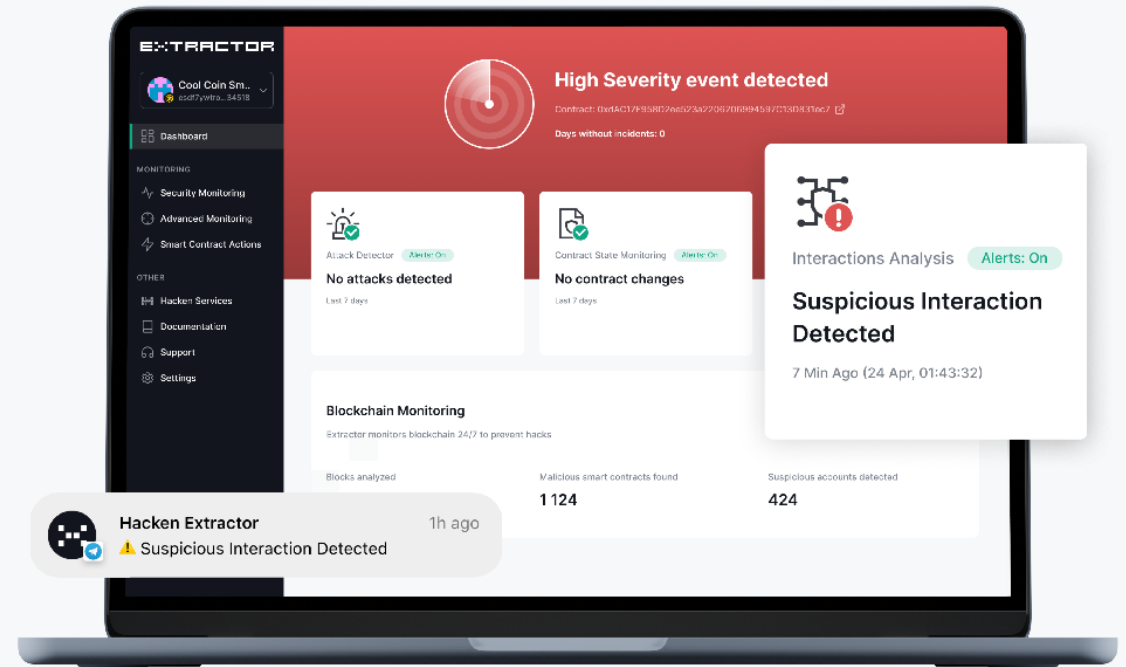
Q1 2024

Detection

- Forta Network Bots
- Cross-chain (events correlation across different chains)
- GPT tuned Attack Detector
- Automatic labeling
- Visual Editor for Attack Detectors
- Alerts Destinations (Slack, Discord, WebHook)

Q2 2024

Protection

- Advanced Scoring (multiple levels based reactions)
- Complex Protection Flow (multi-call, multiple transactions)
- Firewall Contract Level 3
- Mempool frontrunning Level 2
- Dynamic Black list By Hacken
- Tokenomics (Circulation Supply, TVL)
- Social (Twitter, Telegram)
- DeFi (Positions, Liquidity)

Q3 2024

Scale

- EVM chains integration
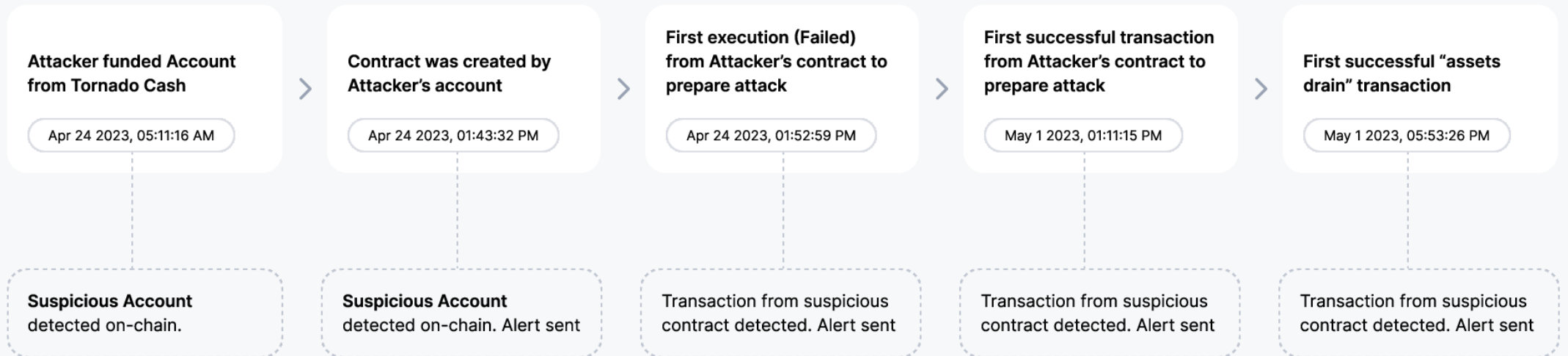- Non-EVM chains integration

Q4 2024

Performance

- Cross Chain Intelligence
- CER Integration
- Fraud Proof Validation
- Threat modeling improvement
- Enhance Incident Response Analysis

Tuesday, May 2, 2023 $1.1M in referral rewards were robbed from the BSC-based perps platform.

Attacker funded Account from Tornado Cash

Apr 24 2023, 05:11:16 AM

Suspicious Account detected on-chain.

Contract was created by Attacker's account

Apr 24 2023, 01:43:32 PM

Suspicious Account detected on-chain. Alert sent

First execution (Failed) from Attacker's contract to prepare attack

Apr 24 2023, 01:52:59 PM

Transaction from suspicious contract detected. Alert sent

First successful transaction from Attacker's contract to prepare attack

May 1 2023, 01:11:15 PM

Transaction from suspicious contract detected. Alert sent

First successful "assets drain" transaction

May 1 2023, 05:53:26 PM

Transaction from suspicious contract detected. Alert sent

If Hacken Extractor was in place, it would prevent hack 7 days beforehand and save $1.1M funds

Attacker funded Account from Tornado Cash

Apr 24 2023, 05:11:16 AM

Contract was created by Attacker's account

Apr 24 2023, 01:43:32 PM

First execution (Failed) from Attacker's contract to prepare attack

Apr 24 2023, 01:52:59 PM

First successful transaction from Attacker's contract to prepare attack

May 1 2023, 01:11:15 PM

First successful "assets drain" transaction

May 1 2023, 05:53:26 PM

Suspicious Account detected on-chain.

Suspicious Account detected on-chain. Alert sent

Offering security audit and post-audit security monitoring as essential services.

For Middle and Small Web3 companies that want to increase level of protection without compromising their roadmap.

Extractor Experts have created and constantly updating the templates of best monitoring and protection functions to make the setup process smooth and effortless

140
Beta Users

100+
Smart Contracts Secured

10
Annual Clients within first month

Time

15 months

Cost

$2 mln

Purpose

Building integrated modules for a swiss-cheese defence model

Expanding Capabilities

Detection of complex long-range attacks across multiple chains

EXTRACTOR

Extractor is poised to be a game-changer in securing the Web3 landscape

Join us in making Web3 a safer place!