HACKING TIME
BY SLOWMIST

WEB3

Security and Compliance

SLOWMIST SLOWMIST AML MISTTRACK MISTEYE

The Battleground of Smart Contracts: How to Outsmart Hackers?

Rebound
TenArmor

About TenArmor

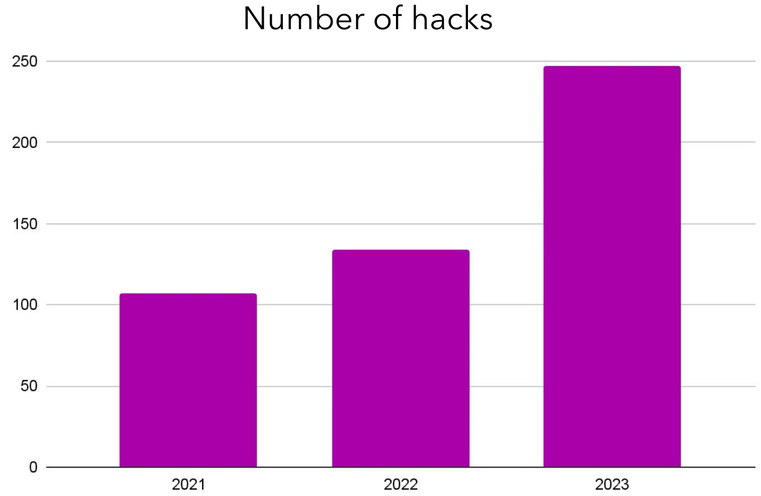
Your Trusted Partner in On-Chain Security

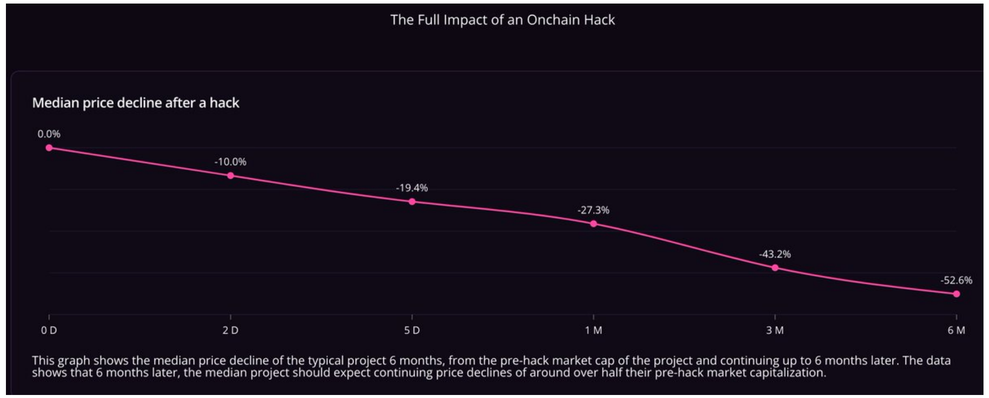
- Intro to TenArmor
  - TenArmor is a Web3 security-focused startup specializing in **real-time on-chain monitoring and response, smart contracts audits, and address screening** services.
  - Since July 2024, We've proactively detected **22503** security incidents(attacks and scams) early with an approximate total loss of **$3.1B.**
  - Successfully recovered **$960k** for projects
- About Rebound
  - Years of experience in Web2 security, now focusing on building Web3 security.

The Current State of Web3 Threats

Identifying the Risks in an Evolving Blockchain Ecosystem

- DeFi: A Prime Target of Hackers





- We need more innovative and proactive solutions

Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- Real-Time Attack Detection and Response
  - **Audits are Essential, but Not a Sliver Bullet**
    - Traditional audits can't identify all vulnerabilities, especially operational or configuration-related issues.
  - **Opportunity to Minimize Losses**
    - Many smart contract exploits involve multiple transactions over hours, providing a window for intervention.
  - **Proactive Defense is Key**
    - Early attack detection and automated responses are crucial to prevent or reduce potential losses.

Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- Many major incidents last multiple transactions and span minutes to hours

Project	Loss	Date	Audit Status	Attack Tx Count	Attack Duration	Reference
Onyx	$4M	2024-09-26	Audited, Bug Bounty Program	**5**	**8 hours**	https://tenarmor.com/blogs/en/
Penpie	$27M	2024-09-03	Audited by WatchPug and Tokyo	**4**	**50 minutes**	https://tenarmor.com/blogs/en/
Ronin Bridge	$11.8M	2024-08-06	Misconfiguration	**3**	**38 minutes**	https://tenarmor.com/blogs/en/
LI.FI.	$11M	2024-07-16	Audited, except for the newly deployed GasZipFacet	**19**	**48 minutes**	https://tenarmor.com/blogs/en/

Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- Project X Successfully Recovered $130K (2024-09-26)

Chain ID	Attacker	Attack Contract	Tx Hash	Loss USD Amount	Block Number	Vulnerability	IOD	Risk Level	Detection Time
BSC	0x0e66..66b5	0xaeb6..dcdf	0x5902..88eb	2.2K	42587591	Business Logic Flaw	1	Medium	6 months ago (2024-09-26 09:22:19)
BSC	0xd4f0..4d62	0x5100..5762	0x665a..39df	6.1K	42584092	Business Logic Flaw	1	High	6 months ago (2024-09-26 06:27:22)
BSC	0xa747..3188	0xaa01..f1b2	0x9dfc..aae9	4.1K	42583982	Business Logic Flaw	1	Medium	6 months ago (2024-09-26 06:21:52)
BSC	0x5b98..bbe6	0x6856..793e	0x5f21..15eb	3.6K	42583599	Business Logic Flaw	1	Medium	6 months ago (2024-09-26 06:02:43)
BSC	0x0e66..66b5	0xaeb6..dcdf	0xde31..61e8	10.8K	42583543	Business Logic Flaw	1	Critical	6 months ago (2024-09-26 05:59:55)
BSC	0xd4f0..4d62	0x5100..5762	0x633f..ece5	5.1K	42583273	Business Logic Flaw	1	High	6 months ago (2024-09-26 05:46:25)
BSC	0x7eda..db8f	0x3e5a..ea47	0x140c..80d2	8.5K	42583039	Business Logic Flaw	1	High	6 months ago (2024-09-26 05:34:43)

Total Loss: 40.4K Total: 7 1 20 items

Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- Project X Successfully Recovered $130K (2024-09-26)

Timestamp:	186 days ago (Sep-26-2024 05:34:43 AM UTC)
Transaction Action:	Call 0x70f51505 Method by 0x7EDaF26b...196d1db8f on 0x3E5Ac0Ca...3B456Ea47
Sponsored:	coinzilla Place your AD here
From:	0x7EDaF26b40f07Ee0110255BB2084Af3196d1db8f
Interacted With (To):	0x3E5Ac0Ca2f9285592fAAf835F648a943B456Ea47
BEP-20 Tokens Transferred: 3	All Transfers / Net Transfers

- From 0x685623DB...4F3D1793E To 0x3E5Ac0Ca...3B456Ea47 For 50,007 $1,600.47 Scallop (SCLP)
- From 0x3E5Ac0Ca...3B456Ea47 To 0x7EDaF26b...196d1db8f For 50,007 $1,600.47 Scallop (SCLP)
- From 0x3E5Ac0Ca...3B456Ea47 To 0x7EDaF26b...196d1db8f For 0 $0.00 Wrapped BNB (WBNB)

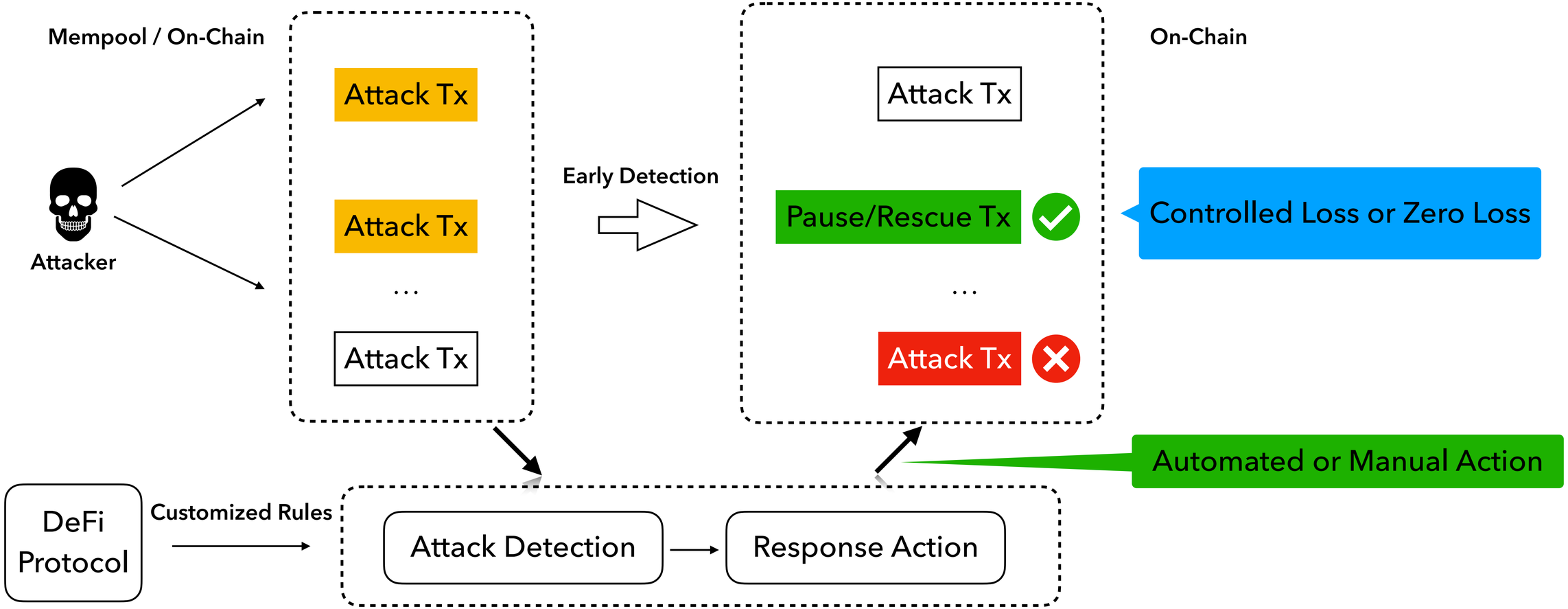
```
function withdraw(address who, uint256 amount) public nonReentrant updateReward(who) {
    require(amount > 0, "Cannot withdraw 0");
    require(block.timestamp > unStakeDate[who], "can't withdraw before withdraw date");
    _totalSupply = _totalSupply.sub(amount);
    _balances[who] = _balances[who].sub(amount);
    stakingToken.safeTransfer(msg.sender, amount);

    emit Withdrawn(who, amount);
}

function getReward() nonReentrant updateReward(msg.sender)  public   {
     uint256 reward = rewards[msg.sender];
    if (reward > 0) {
        rewards[msg.sender] = 0;
        rewardsToken.safeTransfer(msg.sender, reward);
        emit RewardPaid(msg.sender, reward);
    }
}

function withdrawBalance (address who, uint256 amount) payable public onlyOwner{
    require(block.timestamp>1726993171, "Owner cannot withdraw tokens until staking period ends");
    rewardsToken.safeTransfer(who, amount);
    emit withdrawnBalance(who, amount);
}
```

0x6ed50ba1c7...	Withdraw Bal...	42588342	186 days ago	0x685623DB...4F3D1793E	OUT	0x660D5D42...9cfb0eFB7	932	Scallop (SCLP)
0xfde10f50995...	Withdraw Bal...	42588305	186 days ago	0x685623DB...4F3D1793E	OUT	0x660D5D42...9cfb0eFB7	770,000	Scallop (SCLP)
0x607945ba79...	Withdraw Bal...	42587941	186 days ago (2024-09-26 9:39:49)	0x685623DB...4F3D1793E	OUT	0x660D5D42...9cfb0eFB7	0	Scallop (SCLP)
0x274e4e3f95a...	Withdraw	42587916	186 days ago	0x685623DB...4F3D1793E	OUT	0x5B981e4b...9B8c8BBE6	968.805	Scallop (SCLP)
0x33efda8b374...	Withdraw	42587675	186 days ago	0x685623DB...4F3D1793E	OUT	0x5B981e4b...9B8c8BBE6	686.049	Scallop (SCLP)
0x59027299c9...	0xbf4a8476	42587591	186 days ago	0x685623DB...4F3D1793E	OUT	0xaEb68De8...70aaBDcDF	12,723.837	Scallop (SCLP)
0x74026ca676...	0x009489d6	42584903	186 days ago	0x685623DB...4F3D1793E	OUT	0xE2282257...37a0F4150	18,123.415	Scallop (SCLP)

Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- Real-Time Attack Detection and Response



Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- AI-Based Detection Model

TenArmorAlert
@TenArmorAlert

🚨TenArmor Security Alert🚨

Our system has detected a suspicious attack involving #SIR.trading @leveragesir on #ETH, resulting in an approximately loss of $353.8K.

The stolen funds have been deposited into RailGun.

Attack transaction: etherscan.io/tx/0xa05f047dd...

x.com/leveragesir/st...

With TenArmor's TenMonitor, you get early detection and automated response to on-chain attacks.

Need protection? Reach out anytime!

#TenArmorAlert #TenArmor

attack_detection #1263518

createTimestamp: 2 days ago (2025-03-30 06:21:18)

labels: [redacted]

sender: 0x27defcfa6498f957918f407ed8a58eba2884768c

contractAddr: 0xea55fffae1937e47eba2d854ab7bd29a9cc29170

txHash: 0xa05f047ddfdad9126624c4496b5d4a59f961ee7c091e7b4e38cee86f1335736f

blockNum: 22157900

score: 2720

eoasProfit: 354822

Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

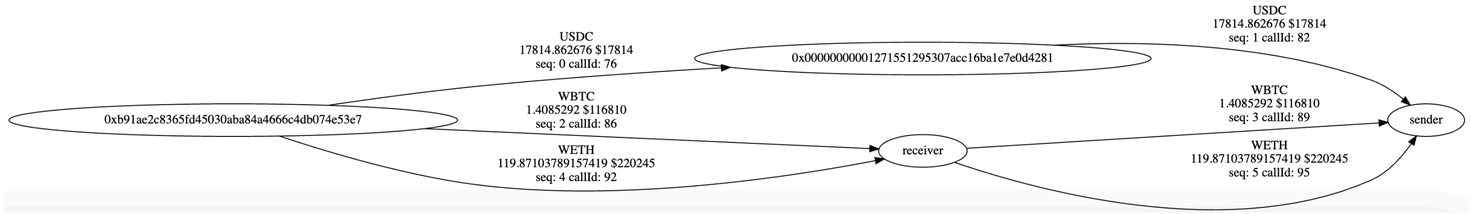
- AI-Based Detection Model
  - Simulates transactions and checks for abnormal fund flow

Balance Changes

```
maxValue: 354822                    maxValueAddr: 0x27defcfa6498f957918f407ed8a58eba2884768c
minValue: -354869                   minValueAddr: 0xb91ae2c8365fd45030aba84a4666c4db074e53e7
```

Address	Token	Amount	Value	Summary
0x000000000001271551295307acc16ba1e7e0d4281	0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48	0	0	inValue: 0 outValue: 0 profit: 0
0x27defcfa6498f957918f407ed8a58eba2884768c	0x2260fac5e5542a773aa44fbcfedf7c193bc2c599 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48 0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	140852920 17814862676 119871037891574190000	116810 17814 220245	inValue: 354869 outValue: 0 profit: 354822
0xb91ae2c8365fd45030aba84a4666c4db074e53e7	0x2260fac5e5542a773aa44fbcfedf7c193bc2c599 0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48 0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	-140852920 -17814862676 -119871037891574190000	-116810 -17814 -220245	inValue: 0 outValue: -354869 profit: -354869
0xea55fffae1937e47eba2d854ab7bd29a9cc29170	0x2260fac5e5542a773aa44fbcfedf7c193bc2c599 0xc02aaa39b223fe8d0a0e5c4f27ead9083c756cc2	0 0	0 0	inValue: 0 outValue: 0 profit: 0

resMsg: Show



Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

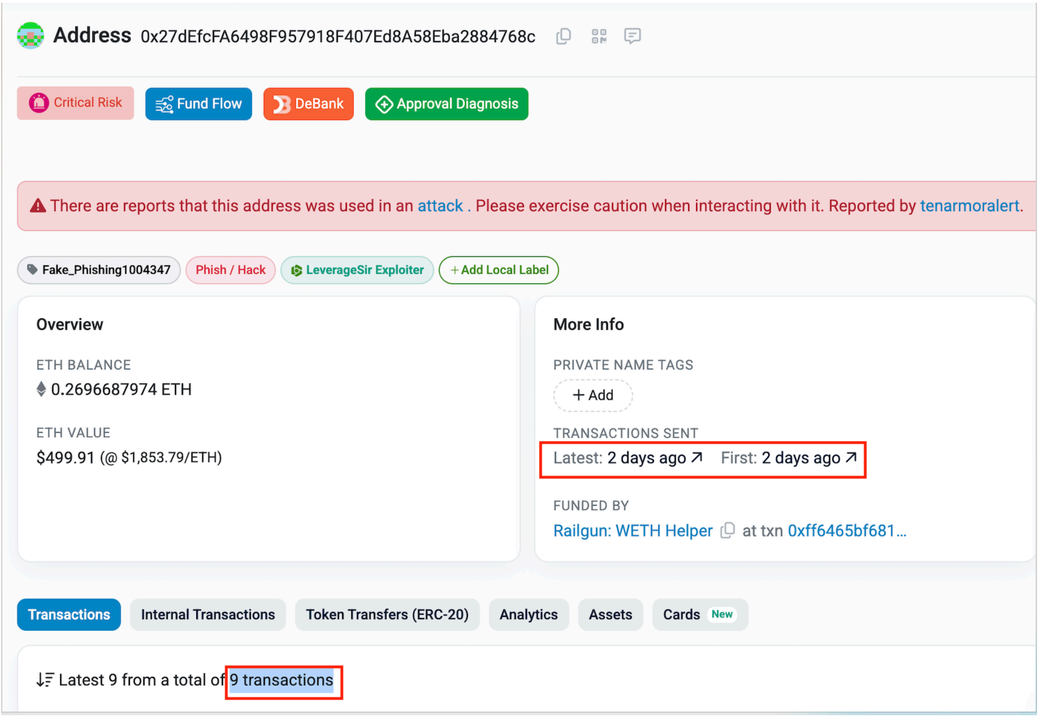
- AI-Based Detection Model
  - Checks for abnormal behavior in call traces

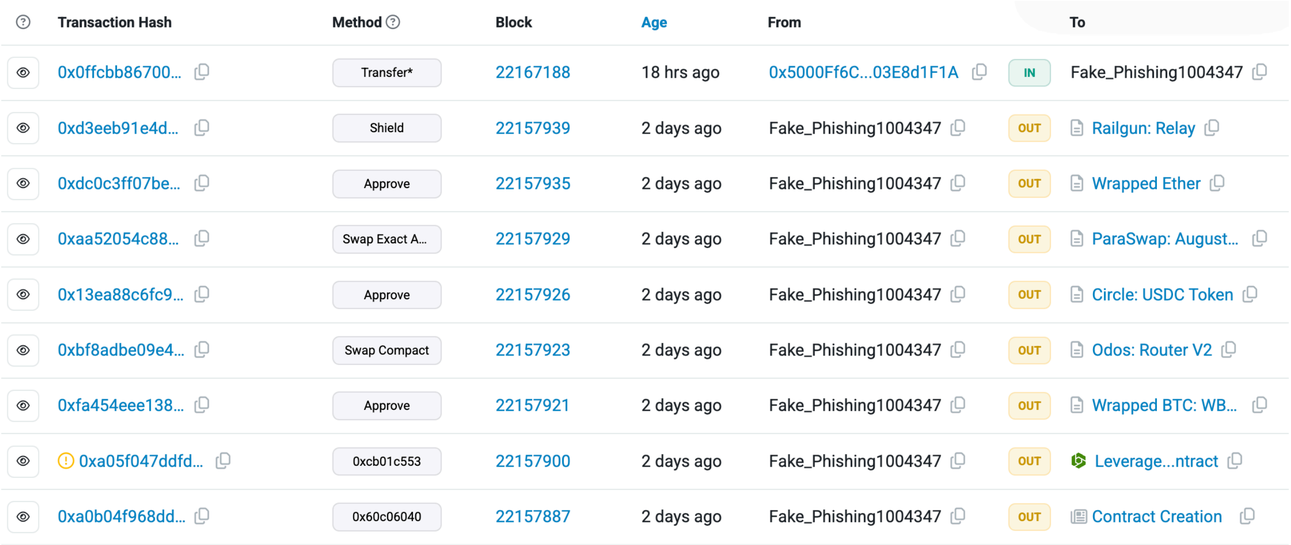
Ether Price:	$1,807.48 / ETH
Gas Limit & Usage by Txn:	26,048,285 | 25,754,539 (98.87%)
Gas Fees:	Base: 0.352720752 Gwei
Burnt Fees:	🔥 Burnt: 0.009084160363493328 ETH ($16.83)

Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- AI-Based Detection Model
  - Checks for abnormal behavior in call traces





Transaction Hash	Method	Block	Age	From		To
0x0ffcbb86700...	Transfer*	22167188	18 hrs ago	0x5000Ff6C...03E8d1F1A	IN	Fake_Phishing1004347
0xd3eeb91e4d...	Shield	22157939	2 days ago	Fake_Phishing1004347	OUT	Railgun: Relay
0xdc0c3ff07be...	Approve	22157935	2 days ago	Fake_Phishing1004347	OUT	Wrapped Ether
0xaa52054c88...	Swap Exact A...	22157929	2 days ago	Fake_Phishing1004347	OUT	ParaSwap: August...
0x13ea88c6fc9...	Approve	22157926	2 days ago	Fake_Phishing1004347	OUT	Circle: USDC Token
0xbf8adbe09e4...	Swap Compact	22157923	2 days ago	Fake_Phishing1004347	OUT	Odos: Router V2
0xfa454eee138...	Approve	22157921	2 days ago	Fake_Phishing1004347	OUT	Wrapped BTC: WB...
0xa05f047ddfd...	0xcb01c553	22157900	2 days ago	Fake_Phishing1004347	OUT	Leverage...ntract
0xa0b04f968dd...	0x60c06040	22157887	2 days ago	Fake_Phishing1004347	OUT	Contract Creation

Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- AI-Based Detection Model
  - Checks for abnormal behavior in call traces

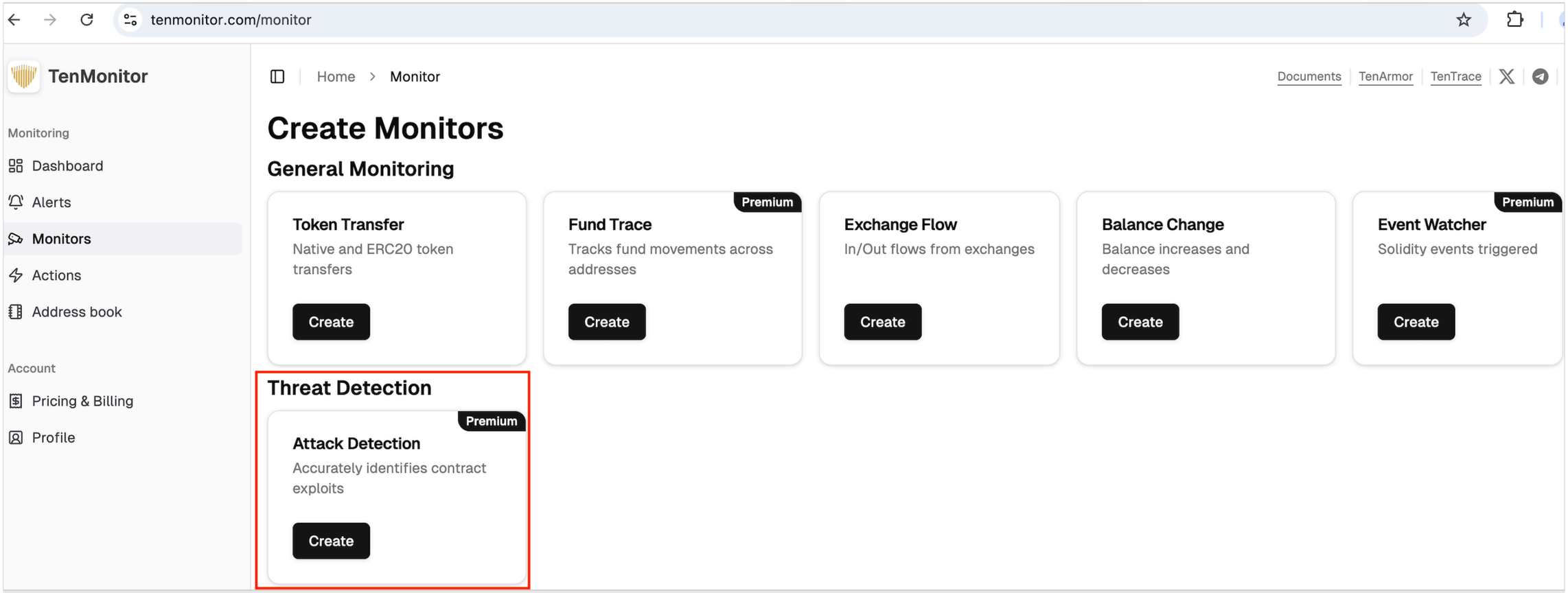
```
[Sender] 0x27defcfa6498f957918f407ed8a58eba2884768c
0 → CALL [Receiver] A.0xcb01c553(raw data) ▸ ()
  1 → CREATE B ▸ (raw data)
  1 → CALL B.mint Calldata(_mintAmount=(long param)) ▸ ()
  1 → CALL B.approve Calldata(spender=Vault, amount=(long param)) ▸ (true)
  1 → EVENT [Receiver] A.Transfer Calldata(from=Null Address, to=[Receiver]A, value=(long param))
  1 → EVENT [Receiver] A.Approval Calldata(owner=[Sender]0x27defcfa6498f957918f407ed8a58eba2884768c, spender=Vault, value=(long param))
  1 → CALL Uniswap V3: Positions NFT.createAndInitializePoolIfNecessary Calldata(token0=B, token1=[Receiver]A, fee=100, sqrtPriceX96=79,228,1
  1 → CALL B.approve Calldata(spender=Uniswap V3: Positions NFT, amount=108,823,205,127,466,839,754,387,550,950,703) ▸ (true)
  1 → CALL [Receiver] A.approve Calldata(spender=Uniswap V3: Positions NFT, amount=108,823,205,127,466,839,754,387,550,957,989) ▸ (true)
  1 → CALL Uniswap V3: Positions NFT.mint Calldata(params=[token0=B, token1=[Receiver]A, fee=100, tickLower=-190,000, tickUpper=190,000, amou
  1 → CALL [Receiver] A.approve Calldata(spender=Uniswap V3: Router, amount=(long param)) ▸ (true)
  1 → CALL Uniswap V3: Router.exactInputSingle Calldata(params=[tokenIn=[Receiver]A, tokenOut=B, fee=100, recipient=[Receiver]A, deadline=1,74
  1 → CALL Vault.initialize Calldata(vaultParams=[debtToken=B, collateralToken=[Receiver]A, leverageTier=0]) ▸ ()
  1 → CALL Uniswap V3: Quoter.quoteExactOutputSingle Calldata(tokenIn=B, tokenOut=[Receiver]A, fee=100, amountOut=114,911,995,060,490,773,496
  1 → CALL Vault.mint Calldata(isAPE=true, vaultParams=[debtToken=B, collateralToken=[Receiver]A, leverageTier=0], amountToDeposit=139,650,998
  1 → CALL Keyless CREATE2 Factory.safeCreate2 Calldata(salt=0x0000000000000000000000000000000000000000d739dcf6ae98b123e5650020, initializati
  1 → CALL 0x000000000001271551295307acc16ba1e7e0d4281.0x11b92ab9(raw data) ▸ ()
  1 → CALL 0x000000000001271551295307acc16ba1e7e0d4281.0x11b92ab9(raw data) ▸ ()
  1 → CALL Vault.uniswapV3SwapCallback Calldata(amount0Delta=0, amount1Delta=140,852,920, data=(long param)) ▸ ()
  1 → CALL Wrapped BTC: WBTC Token.transfer Calldata(_to=[Sender]0x27defcfa6498f957918f407ed8a58eba2884768c, _value=140,852,920) ▸ (true)
  1 → CALL Vault.uniswapV3SwapCallback Calldata(amount0Delta=0, amount1Delta=119,871,037,891,574,186,422, data=(long param)) ▸ ()
```

```
/**
 * @dev This callback function is required by Uniswap pools when making a swap.\n
 * This function is exectuted when the user decides to mint TEA or APE with debt token.\n
 * This function is in charge of sending the debt token to the uniswwap pool.\n
 * It will revert if any external actor that is not a Uniswap pool calls this function.
 */
function uniswapV3SwapCallback(int256 amount0Delta, int256 amount1Delta, bytes calldata data) external {
    // Check caller is the legit Uniswap pool
    address uniswapPool;
    assembly {
        uniswapPool := tload(1)
    }
    require(msg.sender == uniswapPool);

    // Decode data
    (
        address minter,
        address ape,
        SirStructs.VaultParameters memory vaultParams,
        SirStructs.VaultState memory vaultState,
        SirStructs.Reserves memory reserves,
        bool zeroForOne,
        bool isETH
    ) = abi.decode(
            data,
            (address, address, SirStructs.VaultParameters, SirStructs.VaultState, SirStructs.Reserves, bool, bool)
        );

    // Retrieve amount of collateral to deposit and check it does not exceed max
    (uint256 collateralToDeposit, uint256 debtTokenToSwap) = zeroForOne
        ? (uint256(-amount1Delta), uint256(amount0Delta))
        : (uint256(-amount0Delta), uint256(amount1Delta));

    // If this is an ETH mint, transfer WETH to the pool asap
    if (isETH) {
        TransferHelper.safeTransfer(vaultParams.debtToken, uniswapPool, debtTokenToSwap);
    }

    // Rest of the mint logic
    require(collateralToDeposit <= type(uint144).max);
    uint256 amount = _mint(minter, ape, vaultParams, uint144(collateralToDeposit), vaultState, reserves);

    // Transfer debt token to the pool
    // This is done last to avoid reentrancy attack from a bogus debt token contract
    if (!isETH) {
        TransferHelper.safeTransferFrom(vaultParams.debtToken, minter, uniswapPool, debtTokenToSwap);
    }

    // Use the transient storage to return amount of tokens minted to the mint function
    assembly {
        tstore(1, amount)
    }
}
```

Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

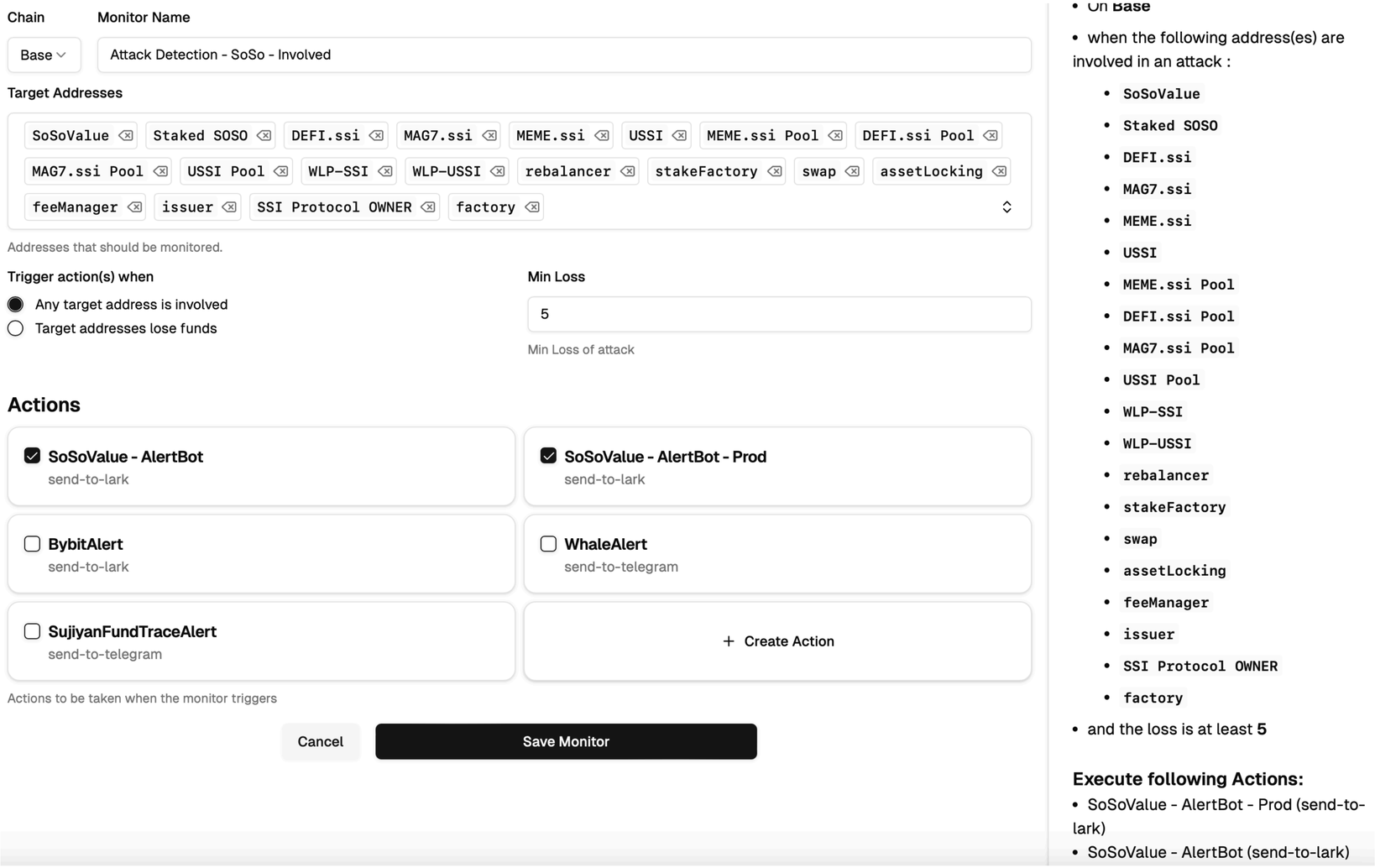
- TenMonitor



Our Solutions to Combat Web3 Threats

Advanced Detection, Response, and Prevention Technologies

- TenMonitor



Key Takeaways for Web3 Protocols

- Security is a continuous process, not a one-time event
- Adopt defense-in-depth, not relying on a single point
  - Audit before launch
  - Monitor after launch
- Respond quickly to incidents to minimize losses
  - Integrate real-time threat detection tools

Thank You for Your Time

- Visit us: www.tenarmor.com
- Email: team@tenarmor.com
- Follow us: @TenArmor, @TenArmorAlert
- Telegram: https://t.me/TenArmorTeam
- TenMonitor: https://tenmonitor.com/
- Securing the future of digital assets – starting with you.