HACKEN + EXTRACTOR

Q3 2024 Web3 Security Report

How much was stolen, and how much could have been saved?

General Trends	**28** The lowest number of hacks in years	**$463.6M** Total value stolen
Recovery Challenges	**94.9%** Worst quarter in funds recovery	**$440.1M** Total lost without recovery
Preventable Exploits	**28.7%** DeFi hacks could have been prevented	**$25.6M** Potential savings with Automated Incident Response

Attack Types

✓ Access control is the most dangerous attack, with losses double all other attacks combined.

✓ Smart contract vulnerabilities most commonly appear after the deployment of new versions.

✓ Rug pulls have declined, but many scammers have shifted to memecoin platforms.

Attack Targets

✓ CEXs are the largest pools targeted by hackers.

✓ Bridges remain the frequent targets for attacks.

✓ Highest share of value lost in Asia.

Preventive Measures

✓

Take Contract Upgrades Seriously

Ensure all smart contract updates are thoroughly audited and tested before deployment to prevent the introduction of new vulnerabilities.

✓

Bug Bounties Are Better Than Forced Bounties

Proactively offer bug bounty programs to incentivize security researchers to report vulnerabilities responsibly, rather than exploiting them.

✓

Implement Automated Incident Response

Deploy real-time monitoring and automated response systems to detect and mitigate attacks swiftly, minimizing potential losses.

✓

Enhance Private Key Security

Use hardware wallets and secure key management solutions to protect private keys from unauthorized access and malware.

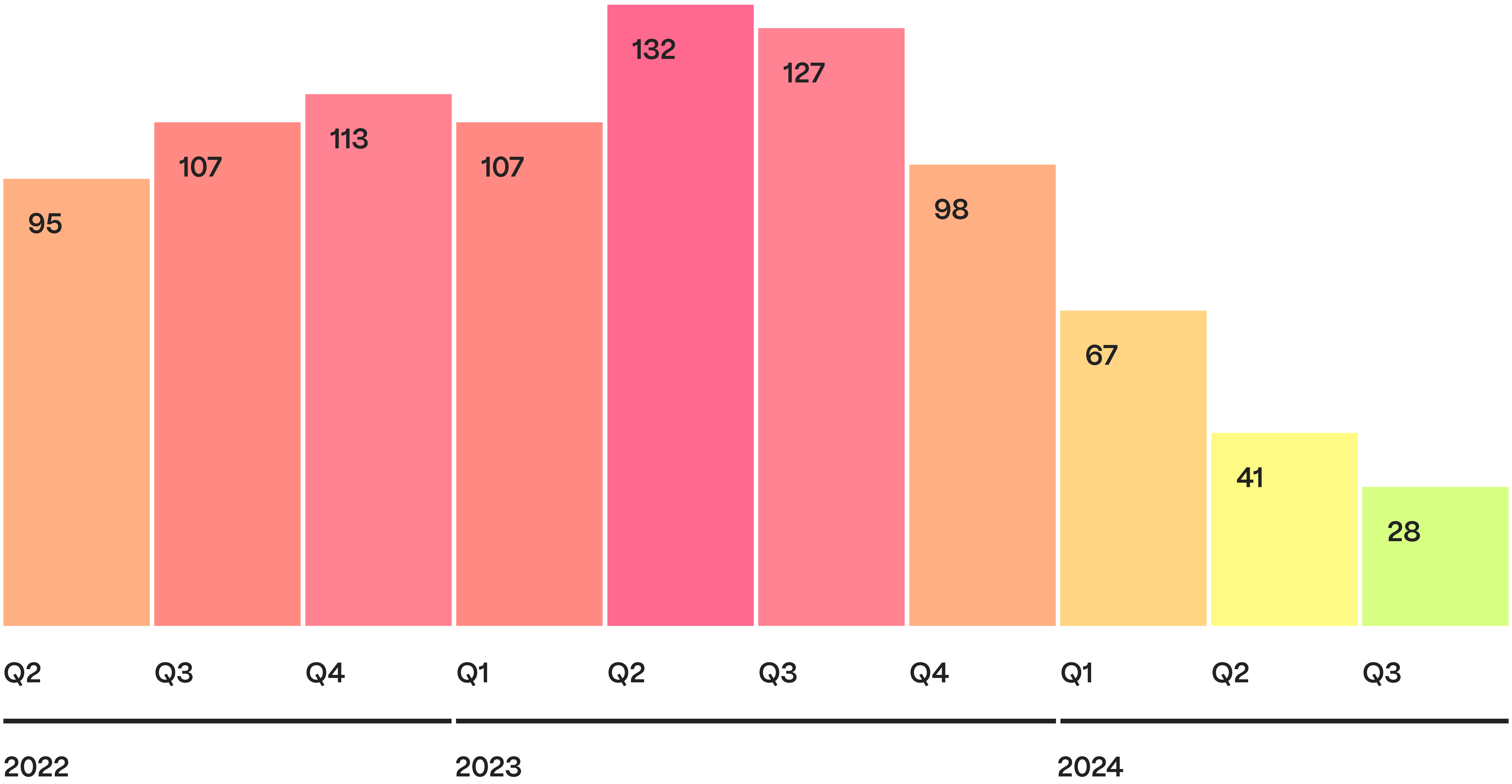
Global Observations

As we wrap up the third quarter of 2024, it's time once again to review the security landscape of the Web3 industry. With increasingly complex technology and layering, it pays to remain vigilant and fully understand the attack vectors as well as the solutions to counter them.

At Hacken, we understand all too well the pain of those who lose digital assets. Liquidity plays a crucial role in most crypto protocols, and losing it is one of the worst things that can happen to a project.

That's why we are pleased to inform you that despite a few high-profile attacks, which we will discuss later, this quarter has seen the lowest number of exploit cases not only this year but also in the past three years.

Number of Incidents per Quarter



A similar trend is observed in the amount of assets stolen, which has been steadily declining throughout the year.

Types of attacks	Q3			Q2		Q1	
	%	Money stolen	Number on incidents	Money stolen	Number on incidents	Money stolen	Number on incidents
Access Control	68.71%	$316,069,000	8	$397,291,000	10	$669,169,089	24
Smart Contract Vulnerability	9.12%	$42,296,000	9	$0	–	$46,768,930	17
Reentrancy	7.27%	$33,460,000	3	$0	–	$0	–
Rug Pull	0.53%	$2,440,000	2	$3,690,000	7	$63,967,879	15
Flash Loan Attack	0.71%	$3,256,000	3	$4,489,000	5	$33,381,776	10
Phishing	12.06%	$55,473,618	1	$0	–	$12,917,550	1
Other	0%	$0	0	$84,358,000	17	$0	0
Oracle Issue	2.30%	$10,600,000	2	$23,100,000	2	$0	0
Total		$463,594,618	28	$512,928,00	41	$826,205,224	67

However, this is the worst quarter in recent times in terms of recovered or frozen funds. Among all the victims, only three projects were able to recover the lost assets. We had hoped that the trend of refunding a percentage of the siphoned funds, which was common in previous quarters, would continue—but alas!

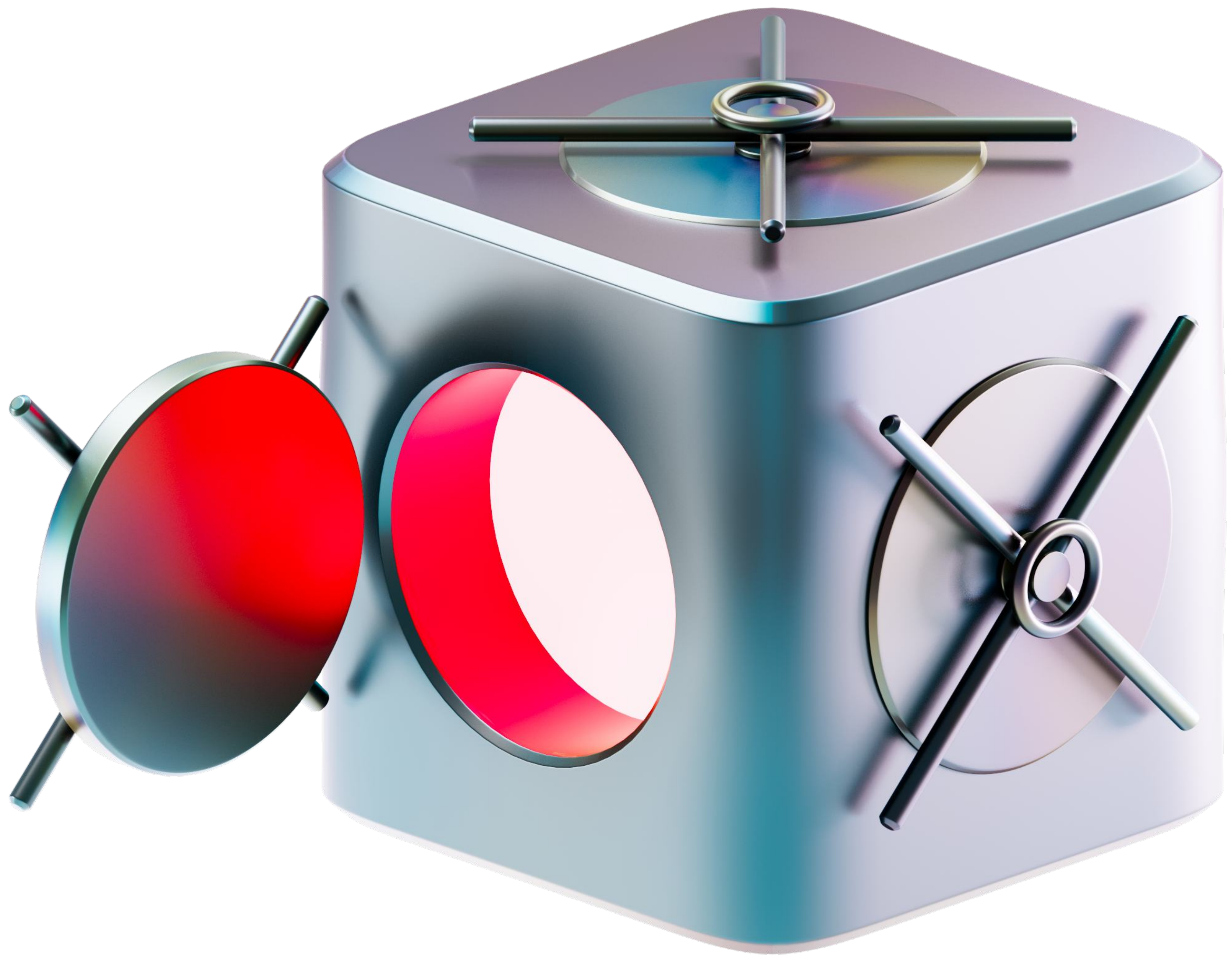
Lost vs Recovered/Frozen Funds	Q3	Q2	Q1
Total Lost	$463,594,618	$512,928,000	$826,205,224
Total Recovered/Frozen	$23,520,000	$347,431,288	$439,533,698
Lost without Recovery	$440,074,618	$165,496,712	$386,671,526

If we look at projects by region, most of the losses this quarter occurred in Asia.

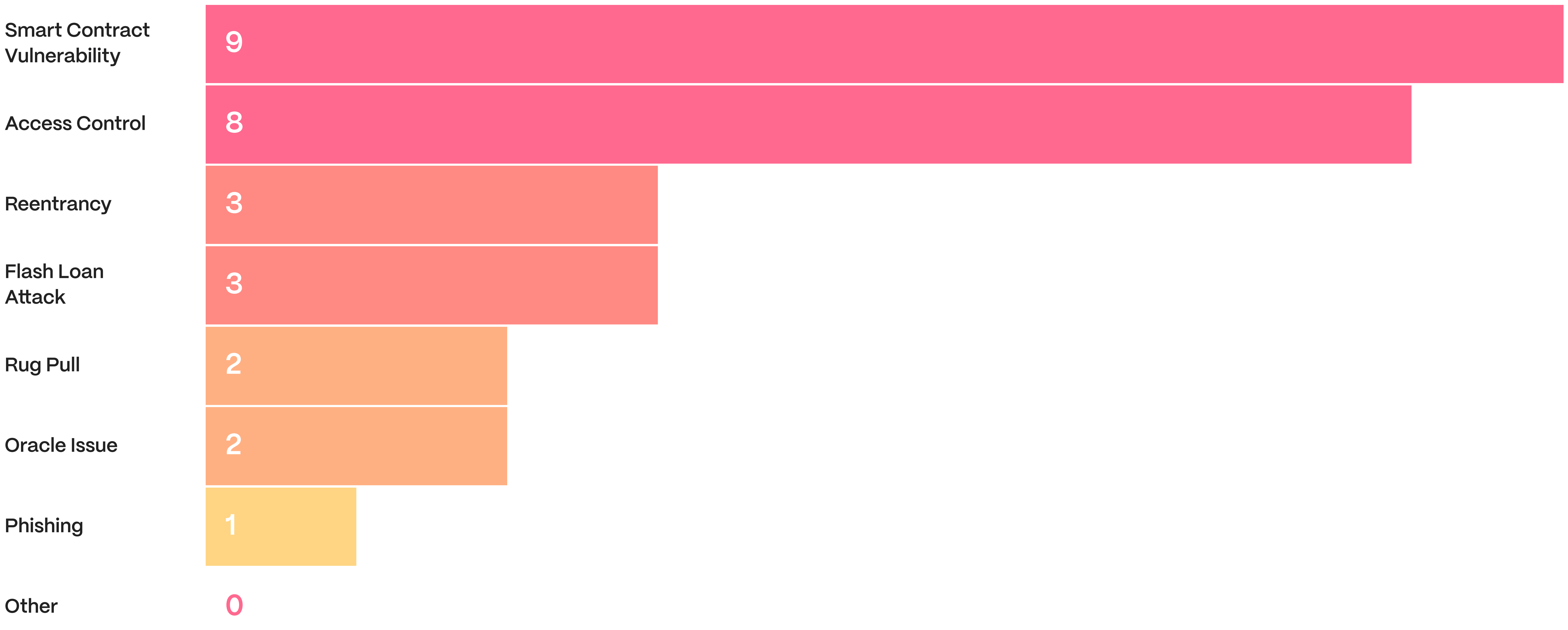
	Q3	
Region	Incidents Per Region	Amount Per Region
Asia	3	$264,000,000
Europe	4	$22,160,000
North America	3	$15,000,000
Australia	1	$43,300,000
Unspecified	17	$119,134,618

Apart from identifying and describing cases of crypto asset theft, we also explored what could be done to prevent larger losses using automated response tools. Our conclusion is that in the DeFi sector alone, at least 28.7% of assets could be frozen as an attack unfolds. The details will be discussed in the following chapters, but for now, let's dive into analyzing what has happened over the last three months.

Attack Types



The total number of attacks saw a notable decline compared to previous quarters, reflecting a positive trend in mitigating the most common vulnerabilities. We attribute this to the Web3 industry reaching a critical mass of robust security solutions and best practices. However, certain attack types remained prevalent, requiring ongoing vigilance and proactive measures.



Total 28

1 Access Control Attacks

As usual, the most damaging type of attack remains the scenario where a malicious actor gains control over the seed or functions, enabling them to arbitrarily withdraw funds from wallets or smart contracts.

With a total of eight cases and $316M stolen, the access control category accounted for more than double the percentage of assets stolen compared to all other attack types combined.

One notable exploit, not typically included in this report but involving an Access Control element, occurred with an unnamed individual using a DeFi Saver proxy. This address became the target of a phishing attack, leading to a change in proxy ownership and a subsequent loss of over $55 million. Although individual fund losses are generally outside the scope of such reports, this case underscores the critical importance of vigilance for anyone in the crypto industry.

Another significant case occurred in mid-September, when several alleged members of the North Korean Lazarus Group infiltrated DeltaPrime, a leveraged farming protocol. They managed to obtain private keys for liquidity pools on Arbitrum and used them to drain $6 million in assets. The well-known on-chain analyst ZachXBT linked the individuals who infiltrated the protocol to a group of pseudo-developers using fake IDs to support one another. This fake network is then leveraged to secure employment within a company, where vulnerabilities are exploited from the inside.

WazirX India Access Control Hack

The WazirX India Exchange hack stands out as the largest attack in Q3 2024, with $230 million lost. Despite employing a robust multi-party security system, the exchange suffered a breach due to unauthorized fund movements from their wallets.

WazirX utilized a Gnosis Safe multisig wallet requiring 4 out of 6 signatures for transactions. Five of the keys were managed by WazirX, while the sixth was held by Liminal, a digital asset custody provider. The attacker managed to manipulate the system, obtaining signatures from three WazirX signers and one from Liminal, allowing them to upgrade the wallet to a malicious contract and siphon off the funds.

In the aftermath, both WazirX and Liminal conducted independent audits, each clearing themselves of vulnerabilities. Grant Thornton's audit confirmed no compromise in Liminal's infrastructure, while Mandiant found no evidence of compromise on WazirX's devices. This led to speculation about an inside job, although no concrete evidence supports this theory.

2 Reentrancy & Smart Contract Vulnerabilities

One of the most persistent methods of extracting assets from a protocol is the reentrancy attack. This involves exploiting a loop in a smart contract's withdrawal function, allowing the attacker to withdraw funds multiple times. It is particularly devastating for protocols with liquidity pools.

Although this quarter saw only three reentrancy attacks, they resulted in over $33 million in losses across various assets.

Another significant category of attacks stems from coding errors, design flaws, or inadequate testing of smart contracts, leaving them vulnerable to exploitation. This attack has happened nine times this quarter, leading to nearly the same amount of losses—approximately $42.3 million. Notably, most of these attacks occurred following the deployment of new updates without undergoing proper security audits.

Vow Token	Minterest	Terra Luna
$1.23m Hack	$1.46m Hack	$6.5m Hack
The Vow hack involved a critical error during live testing on the mainnet. The team modified a rate-setting formula, which allowed an attacker to exploit the temporary change and mint excessive tokens. This occurred within the first minute after deployment, suggesting either a targeted vulnerability scan or potential insider involvement.	This hack exploited a reentrancy vulnerability within its smart contracts on the Mantle Network, resulting in a $1.4 million loss. The attacker initiated the exploit by taking out a flash loan, which allowed them to manipulate market exchange rates through the project's mUSDY contract. By leveraging the reentrancy vulnerability, the attacker repeatedly borrowed and converted tokens, accumulating excess mTokens that were then used to drain assets from the protocol. This attack not only exposed weaknesses in price manipulation and reentrancy but also emphasized the importance of comprehensive security audits to prevent such exploits.	This continually struggling blockchain was targeted by a sophisticated exploitation of its Inter-Blockchain Communication (IBC) system. The attacker deployed a malicious CosmWasm contract, exploiting the MsgTimeout function to mint and transfer tokens off the platform. This breach was facilitated by a previously identified and patched vulnerability, but because no proper quality control or audit was done to the new update, it overwritten the old patch and opened the identified vulnerability once more.

3 Rug Pulls vs Memecoins

The decrease in the number of attacks may also be attributed to the decline of traditional rug pull schemes. While this is a positive trend, an important caveat must be noted:

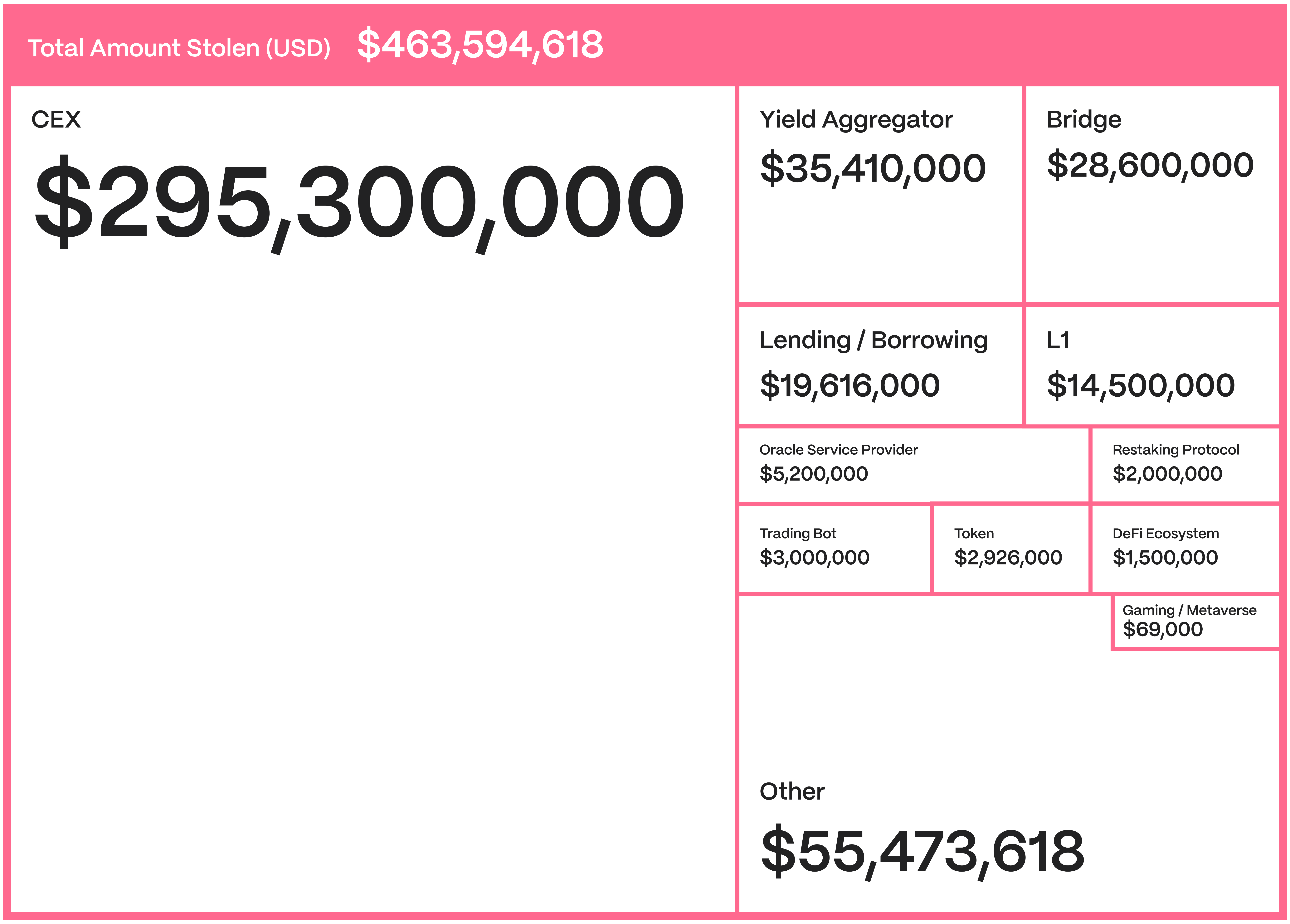
Rug pulls typically involve launching a product, accumulating liquidity in pools, and then removing assets through various means. This behavior is alarmingly similar to that of many memecoins that have emerged on the Base, Tron, and Solana blockchains, coinciding with the disappearance of typical rug pulls.

What is even more concerning is that on Pump.Fun, the largest Solana platform for creating memecoins, over 2 million coins have been launched in recent months, with only 89 of them achieving significant adoption and reaching a market cap of at least $1 million.

This suggests that many perpetrators of rug pull scams may have migrated to these coin factories, where they mimic legitimate activity.

Project Types Affected

With the prevalence of smart contract exploits during this period, it is unsurprising that the DeFi sector was the most common target. Protocols with liquidity pools as part of their architecture are frequently probed by hackers searching for vulnerabilities. Additionally, the complexity and various integrations with other projects often create security gaps, leading to significant capital loss.



Even the largest protocols like Aave may leave its periphery contracts unprotected. This was exactly the case with ParaSwapRepayAdapter that was not included in any audits and exploited by a hacker for $56,000.

Three bridges were hacked – PolyNetwork, LiFi Finance, and the Ronin Bridge, notorious for the largest bridge hack in 2022. This time, however, it netted only $28.7 million – or 6.2% – of total losses among all three.

As noted in previous reports, the two categories that typically lose the most money are CEXes and bridges. This quarter, only three attacks targeted centralized exchanges, yet they accounted for nearly 64% of all funds lost.

Additionally, in the case of Ronin Bridge it was a white hat MEV bot who front-runned exploit transaction, extracting around $12 million in ETH and USDC. The funds were quickly returned, and Sky Mavis awarded the hacker a $500,000 bounty while announcing security improvements to the bridge. Notably, this exploit was introduced by a recent, unaudited update.

Affected Networks

		Chains By Incident Category						
	Incidents Per Network	Access Control	Reentrancy	Smart Contract Vulnerability	Rug Pull	Flash Loan Attack	Phishing	Oracle Issue
Ethereum	17	5	1	8	0	1	1	1
Bitcoin	1	1	0	0	0	0	0	0
Optimism	2	1	0	1	0	0	0	0
Tron	1	1	0	0	0	0	0	0
Polygon	1	1	0	0	0	0	0	0
Mantle	1	0	1	0	0	0	0	0
Base	1	0	0	0	1	0	0	0
Terra Luna	1	0	0	1	0	0	0	0
BNB Chain	4	1	0	0	1	2	0	0
Arbitrum	2	1	0	1	0	0	0	0
PolyNetwork	1	0	1	0	0	0	0	0
Bittensor	1	1	0	0	0	0	0	0
Scroll	1	0	0	0	0	0	0	1
Solana	1	0	0	0	0	0	0	1

We closely monitor the distribution of hacks across various blockchain networks, identifying patterns in attack frequency and type. Overall, vulnerabilities vary across networks, with Ethereum and BNB Chain being the most commonly impacted by a wider range of issues. This analysis serves two crucial purposes:

- ✓ It highlights network-specific vulnerabilities, revealing which attack vectors are more prevalent on particular blockchains.
- ✓ It enables developers and security teams to implement targeted protective measures for smart contracts deployed on these networks.

It’s important to remember that a single attack can target multiple blockchain. Yet, by tracking these trends, we can proactively enhance security protocols and raise awareness about blockchain-specific risks, ultimately contributing to a more robust and resilient decentralized ecosystem.

Incident Prevention in Real Time

Out of $89.8 million lost in DeFi exploits over the Q3, approximately $25.6 million (28.7%) could have been secured with automated incident response strategies.

On-chain monitoring & automated incident response are crucial in understanding and preparing for security threats each project faces.

After analyzing DeFi exploit patterns this quarter, we conclude that a significant share of the lost funds could have been prevented with an Automated Incident Response Strategy.

Automated Incident Response Strategy (in Web3) is a system that utilizes automated tools and predefined actions to identify and counteract security threats in the blockchain ecosystem. It requires a potential threats analysis, determination of the on-chain conditions that flag these threats, and a defined list of automated on-chain actions that should be executed when malicious/highly suspicious on-chain conditions are met.

Exploits are usually not single-transaction hacks but involve a series of transactions with preparation and exploitation phases. In the Aave periphery contract hack, all actions were executed in the same transaction, including the creation of the malicious contract. However, most exploits involve multiple transactions. For example:

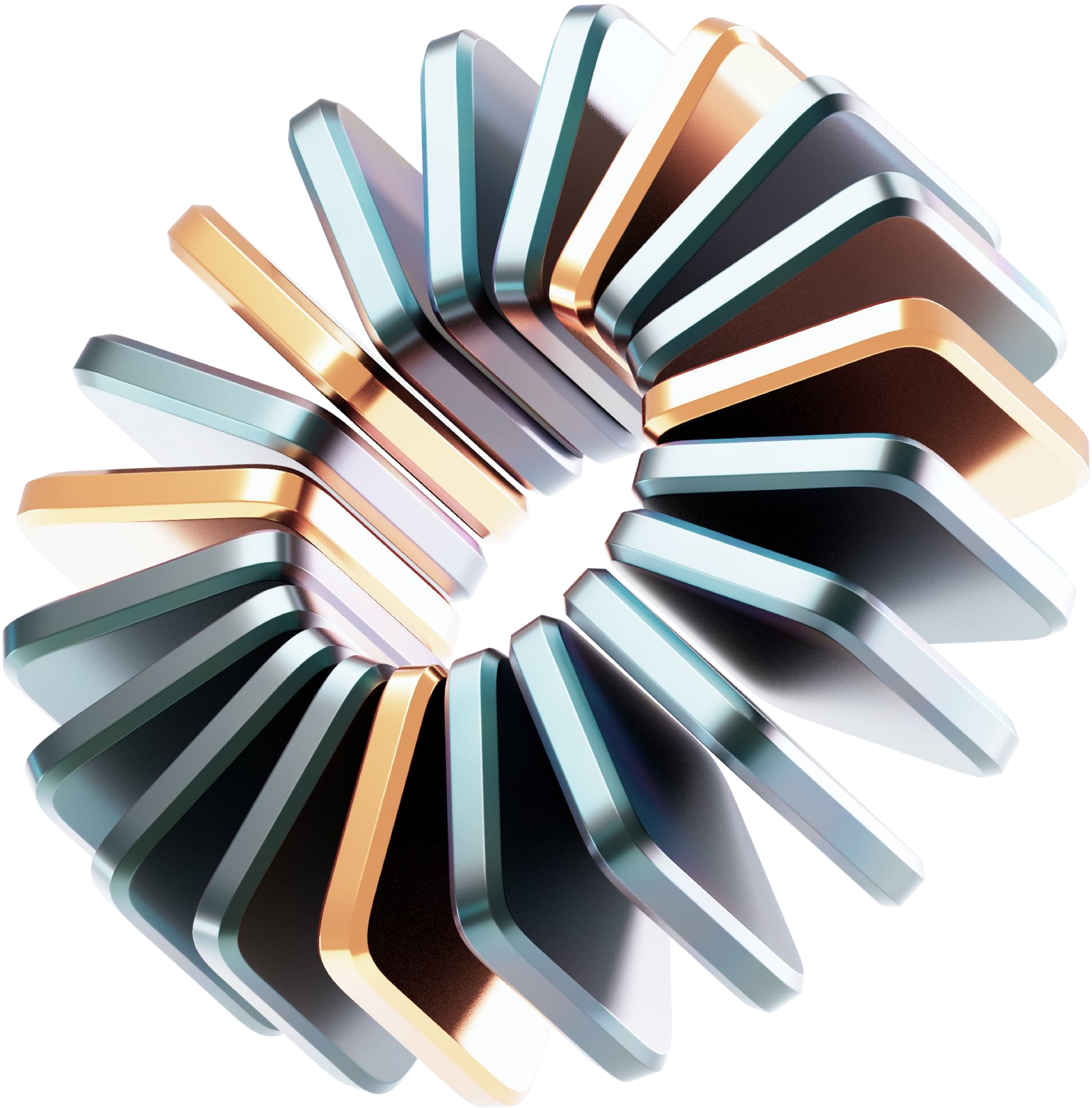
1. attacks with preparatory transactions, where suspicious activity, such as funding from crypto mixers;
2. multi-step exploits, where malicious transactions target different pools one by one;
3. direct exploitation of Access Control through malicious Proxy Upgrade before withdrawing funds

We propose an Automated Incident Response Strategy that can deal with multi-transaction attacks by monitoring on-chain activities and triggering automated actions in response to suspicious or malicious behavior. The analysis will reveal how much could have been saved with this Strategy.

The Automated Incident Response Strategy (AIRS) can be implemented using various techniques and can differ based on the level of customization for each Web3 protocol, as well as the type of on-chain monitoring employed (e.g., monitoring a mempool versus confirmed transactions). In this case, we define a Simplified Automated Incident Response Strategy, where we focus exclusively on confirmed transactions as the on-chain conditions, and the adjustments are made based on general, well-known smart contract behavior patterns rather than highly customized configurations for each protocol.

Automated Incident Response Strategy In Action

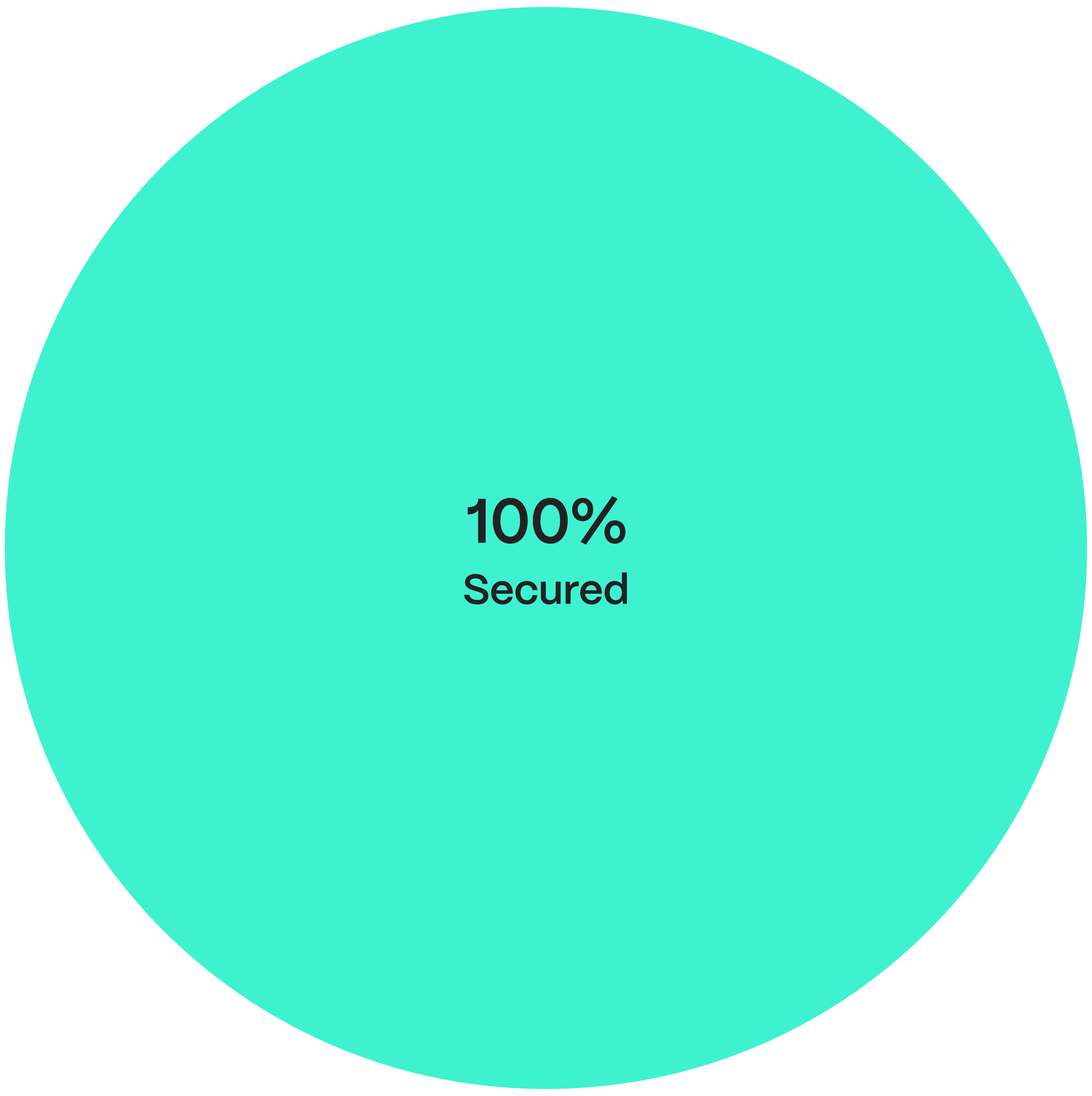
Let's walk through hack cases and analyze them in a way of applying Automated Incident Response Strategy.



Nexera	$1.5m hack
Incident response: 1.5M out of 1.5M Secured	

As the NXRA token contract is upgradable, after pausing the contract, the team managed to burn the frozen tokens on behalf of the attacker's account. In that way, they did not let remaining NXRA tokens to be exchanged for liquid assets such as ETH.

Percentage of the total loss which was possible to secure: 100% ($1.5m)



✓ The exploiter accessed ProxyAdmin contract via the exposed Private Key and upgraded several proxy contracts

✓ Then, the attacker managed to withdraw a total of 47.2M NXRA tokens.

✓ Attacker succeeded at swapping 15M NXRA tokens before the token got paused by the team. The rest of the NXRA tokens remained frozen on the attacker’s wallet

As the NXRA token contract is upgradable, after pausing the contract, the team managed to burn the frozen tokens on behalf of the attacker's account. In that way, they did not let the remaining NXRA tokens be exchanged for liquid assets such as ETH.

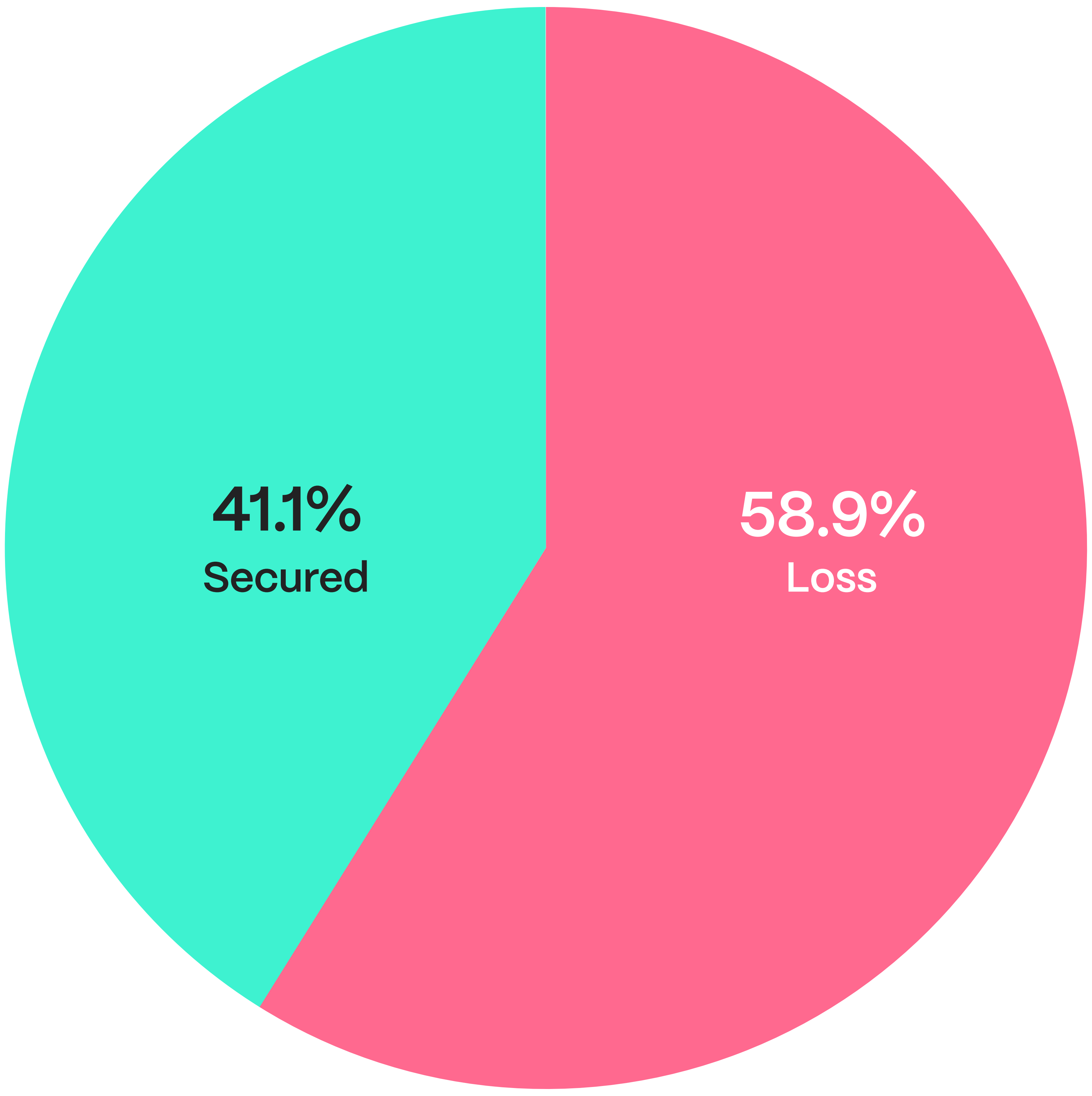
The liquidity in ETH that the attacker managed to withdraw from DEX swapping NXRA tokens is ultimately lost. However, it was possible to prevent this if the Automated action of Pausing the token was configured WHEN the Proxy is maliciously upgraded. Thus, there is no chance for the attacker to swap NXRA for ETH as the token is paused and cannot be transferred.

Penpie	$27m hack

Incident response: 11.1M out of 27M Secured

The attacker exploited a reentrancy vulnerability by creating valueless versions of Pendle's yield-bearing tokens and linking them to valuable assets.

There were 3 major attacks executed which took place on the ETH network. The biggest amount of assets stolen was in the first attack transactions, where the attacker managed to withdraw 15.7m out of 27m total drain.



Percentage of the total loss which was possible to secure: 41% ($11.1m); second and third attack would not happen in that way

attack №	attack tx	executed by	attack time	assets stolen	worth $usd
attack 1	0x56e09	Exploiter 2	06:23:35 PM UTC	2,722.90 wstETH, 2,522,685.57 sUSDe, 1,373.13 agETH, 893.52 rswETH	$15.7m
attack 2	0x42b2e	Exploiter 1	06:37:59 PM UTC	1,367.72 agETH, 901.86 rswETH	$5.6m
attack 3	0x663b5	Exploiter 1	06:42:35 PM UTC	1,359.65 agETH, 899.74 rswETH	$5.5m

Contracts were paused 20 minutes after the first attack was executed.

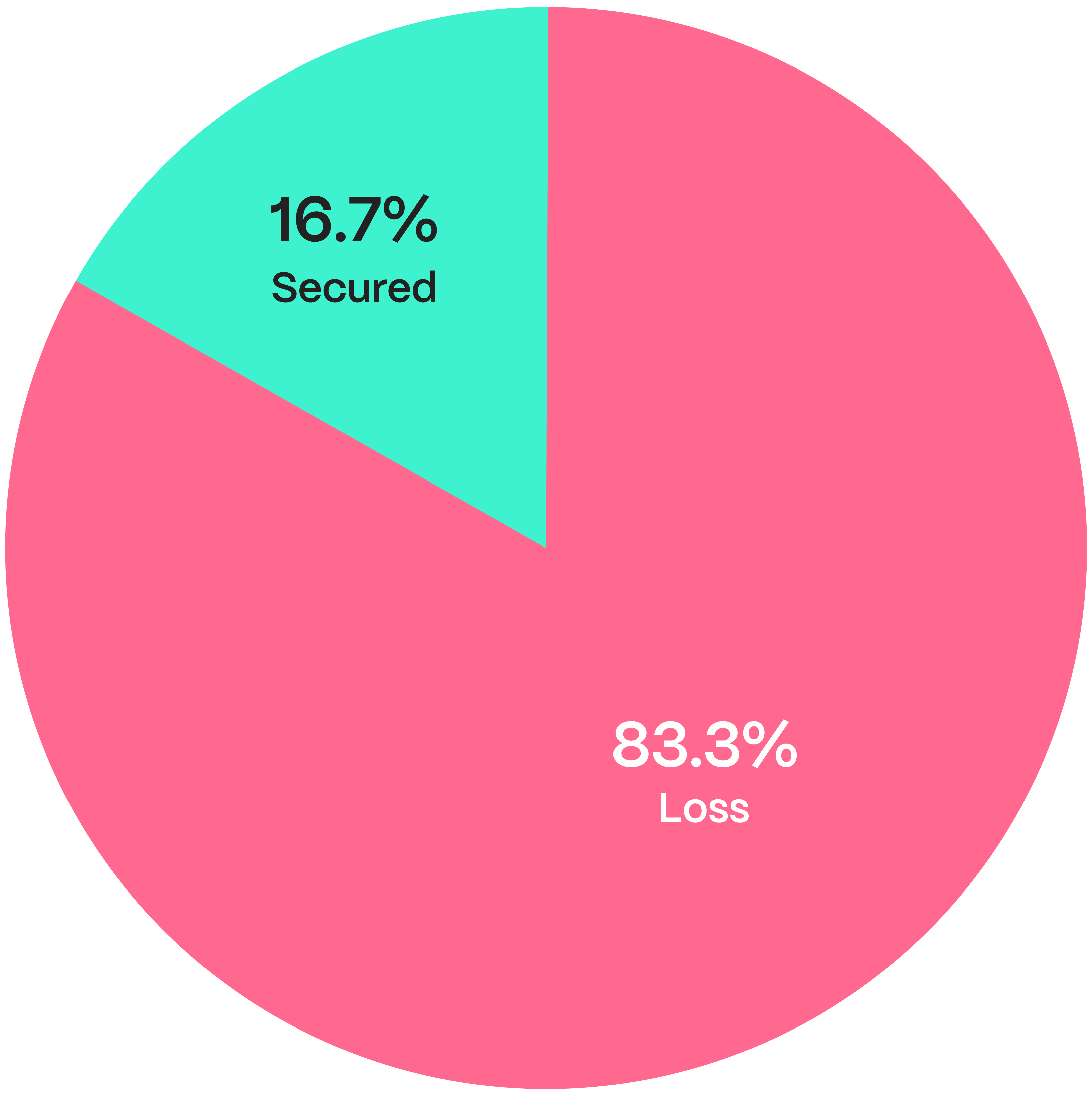
Another key takeaway here is attackers deployed 5 attack contracts, only 3 of them were used in attacks, the 4th attack contract was deployed just 1 minute after Pendle paused their contracts. This fact underscores the importance of timely executed actions in order to respond to the ongoing incident.

The loss of $11.1m was possible to prevent, if Automated action of Pausing contracts was configured WHEN One of the Pools is drained for >50%, which was the case for first attack.

Ronin bridge	$12m hack
Incident response: 2M out of 12M Secured	

Hack occurred due to the issue with the Bridge upgrade. The vulnerability was that the contract was not properly initialized, leaving a critical parameter empty. This oversight allowed attackers (which happened to be white-hat) to withdraw 2M USDC and 4,000 ETH without proper signatures.

Percentage of the total loss which was possible to secure: 17% ($2m)



The timeline of the exploit

9:37 AM UTC
4K ETH withdrawn

10:11 AM UTC
2M USDC withdrawn

10:15 AM UTC
Contract paused

The Bridge was paused 4 minutes after the second withdrawal and 38 minutes after the initial one.

The withdrawal of 2m USDC was possible to prevent*, if Automated action of Pausing contracts was configured WHEN Bridge executes suspicious withdrawal of huge amount of liquidity**

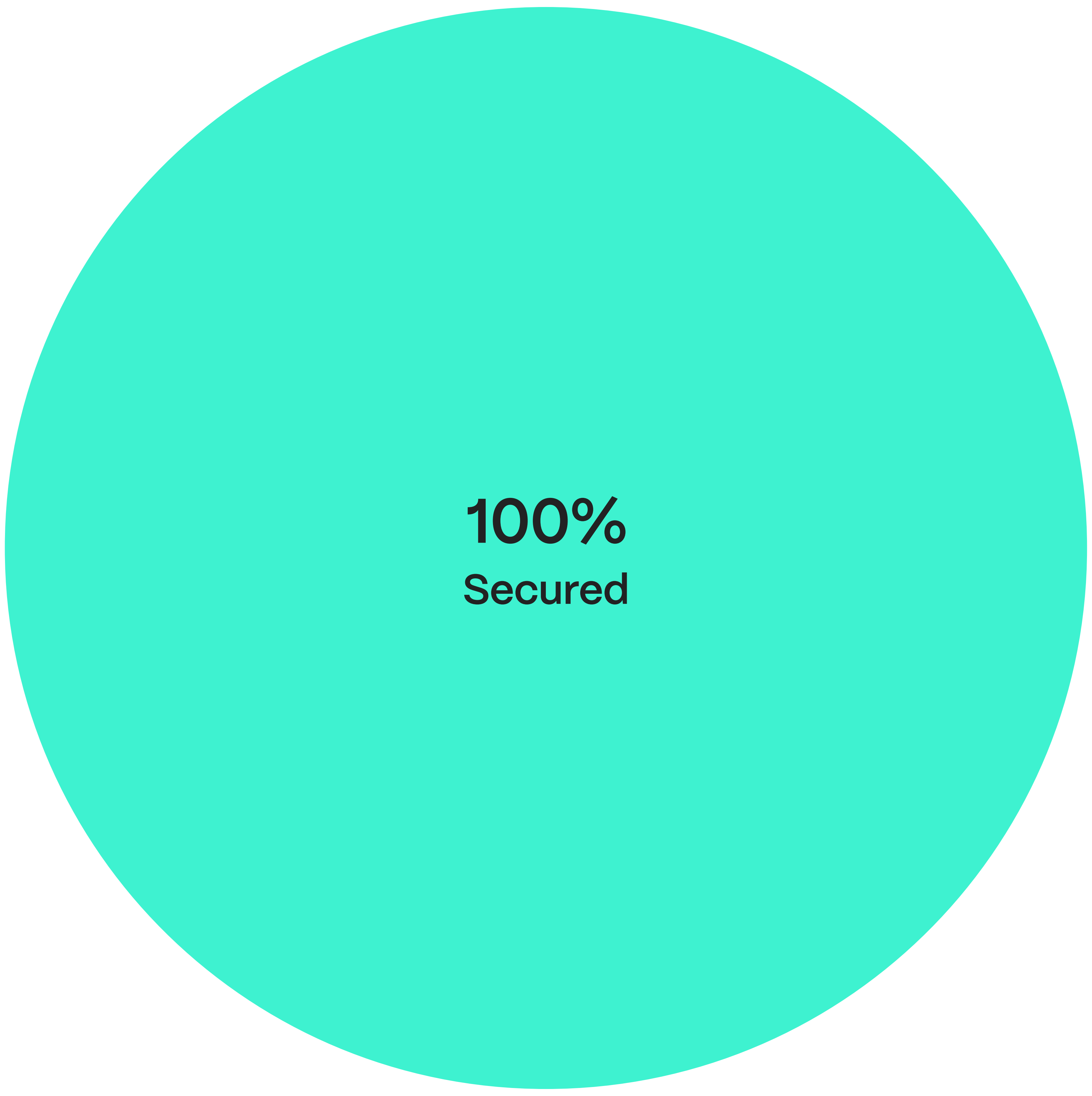
* Here the withdrawal of 2m USDC counts to a total loss, even though it was executed by the white-hats, as it is still assets which were withdrawn as a result of vulnerability.

** The definition of “suspicious withdrawal” refers to the fact that this particular withdrawal of 4K ETH was not a regular one in terms of function call parameters. The fact that it also was of 4K ETH (which is the limit for single-transaction withdrawal) might be determined/flagged as a highly suspicious (or even malicious right due to these facts) transaction. This note is made due to the non-binary nature of the evaluation of malicious transactions.

Onyx	$3.8m hack
Incident response: 100% Secured	

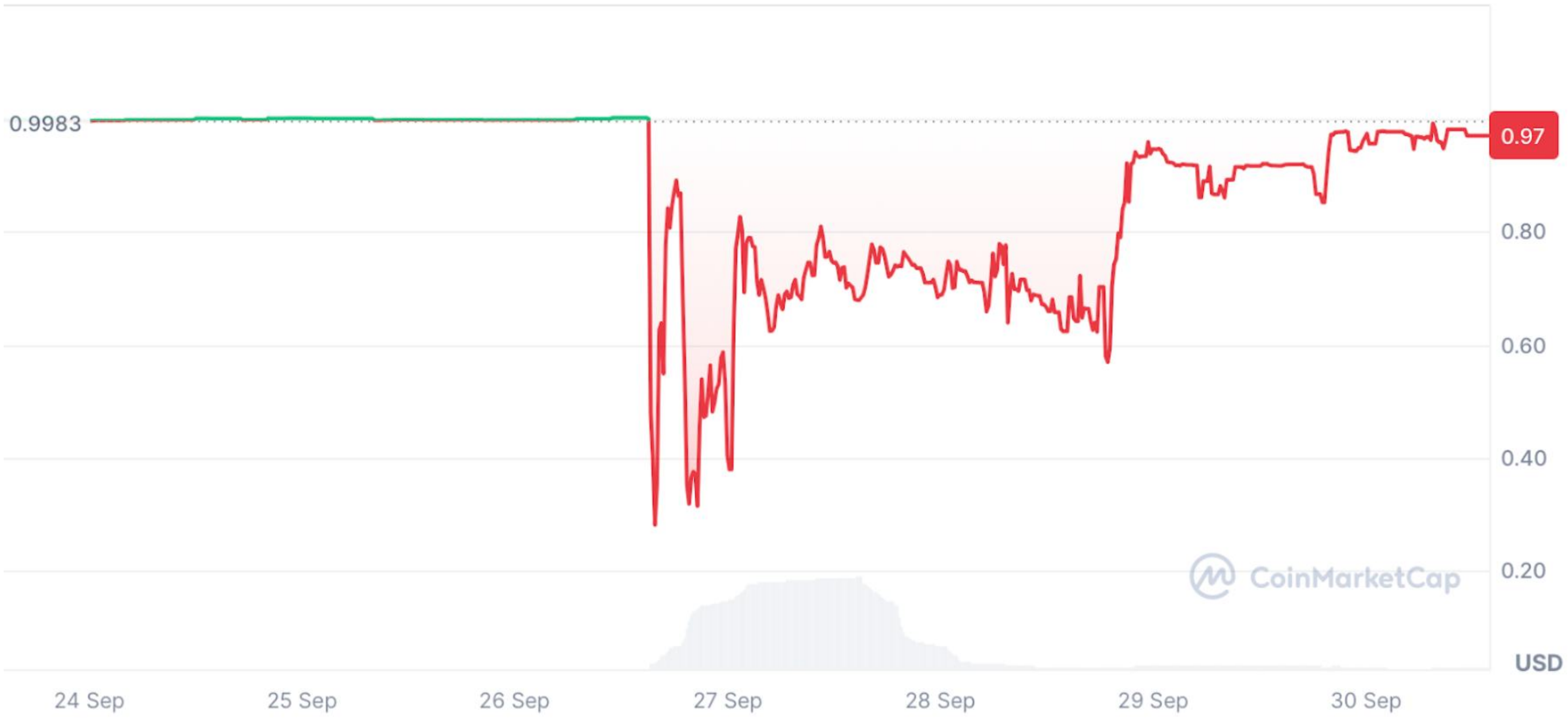
1. The attacker exploited a known precision vulnerability in the Onyx Protocol's forked CompoundV2 code base, which allowed manipulation of the token exchange rate.
2. Once the exchange rate was manipulated, the attacker withdrew approximately 3.8 million VUSD.

Percentage of the total loss which was possible to secure: 100%($3.8m)



Breaking down the timeline of the Onyx exploit, the attacker withdrew 3.8 million VUSD and began exchanging VUSD for ETH just six minutes later. Sixty minutes after the attack took place, the last VUSD to ETH swap was executed.

However, the VUSD stablecoin token contract includes a blacklist functionality, but the exploiter was not blacklisted within those 60 minutes. The 3.8 million VUSD represents 7% of the overall VUSD circulating supply, and the withdrawal of such a percentage is a significant anomaly that should trigger immediate alerts. Upon detecting such an unusual transaction, the system could automatically invoke the blacklist function to prevent the attacker from moving or swapping the stolen VUSD, preventing a significant depeg.



These case studies demonstrate the potential effectiveness of an Automated Incident Response Strategy in mitigating losses during security incidents. While AIRS cannot prevent all types of attacks, it can significantly reduce the impact by enabling automated responses to suspicious activities.

Disclaimer:
It is important to note that the proposed Threat Prevention and Incident Response Strategies are simplified versions of the Strategy adjustment for each of the projects. In reality, protecting Smart Contracts in real time requires thoughtful sophisticated adjustments to each of the Smart Contracts and to the system of the Smart Contract as-is, modeling threats and using different monitoring approaches.

Preventive Measures

1 Audits and Bug Bounties

Despite the losses this quarter, we want to emphasize that the overall security health of the Web3 industry has improved significantly. Avoidable mistakes are less frequent, and companies are generally adhering to best practices for securing their infrastructure. Crypto is maturing, and we hope this positive trend continues.

That's why it's particularly frustrating to see companies making mistakes like deploying updates without proper security audits, only to be hacked within weeks and then seek an audit afterward.

Audits

Audits do make a difference. While they are not foolproof and can sometimes miss issues—as happened with Convergence Finance, one of two instances this quarter where an audited smart contract was hacked—they greatly reduce the likelihood of exploitation in Web3 projects.

Security Measures	Q3	out of
Audited Projects	11	27
Not Audited	16	27
Smart Contract in Audit Scope	2	11

Bug Bounties

Same can be said about bug bounties. Whenever a hack happens, companies often are forced to offer large bounties to return the funds. Each hack is a reputation hit, while having an active bug bounty with clearly defined scope and rewards usually increase a company's reputation in the eyes of their community

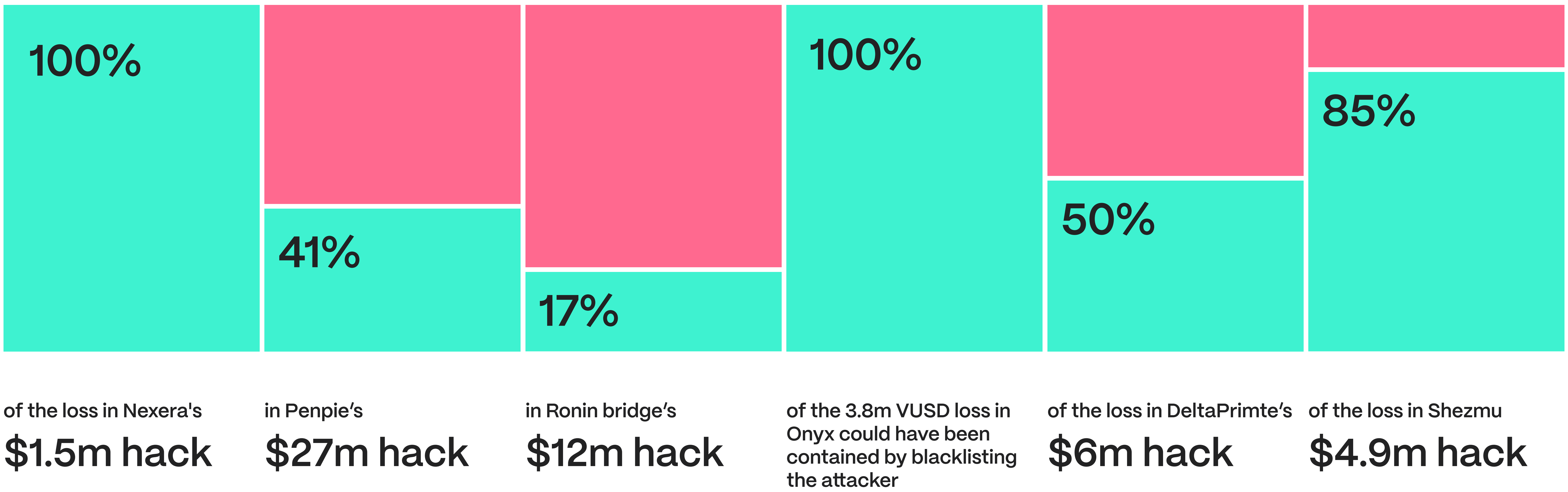
Security Measure	Hacked Projects	Total Hacks
Active Bug Bounty During Attack	7	28
Vulnerability in Bug Bounty Scope	1	28

2 Automated Incident Response Strategies

As we analyze the exploits from this quarter, a clear pattern emerges: many attacks could have been mitigated or prevented through automated incident response strategies. Our analysis indicates that implementing such strategies could have averted at least 28.7% of the DeFi total losses in Q3

Most exploits follow a sequence of transactions, including preparation and exploitation phases. While some, like the Aave periphery contract hack, were executed in a single transaction, the majority involved multiple steps that could have been detected and addressed automatically.

Automated Incident Response Could Have Averted These Hacks



EXTRACTOR

Hacken Extractor offers an on-chain monitoring service that supports all of the **Automated Risk Mitigation and Incident Response Strategies** described above, as well as more **Sophisticated Threat Detection and Prevention Strategies** adjusted specifically to each project in the Web3 space.

Protect Against Social Engineering, Malware, and Phishing Attacks

- ✓ **Enhance Private Key Security**

  Use hardware wallets and secure key management solutions to protect private keys from unauthorized access and malware.

- ✓ **Educate Team Members on Security Best Practices**

  Regularly train staff to recognize and avoid phishing attempts and social engineering tactics that could compromise credentials.

- ✓ **Implement Multi-Factor Authentication (MFA)**

  Require MFA for all sensitive accounts and systems to add an extra layer of security beyond just passwords or private keys.

- ✓ **Conduct Regular Security Audits and Penetration Testing**

  Periodically assess systems for vulnerabilities through professional security audits and penetration tests.

- ✓ **Limit Access Privileges**

  Apply the principle of least privilege by granting employees the minimum levels of access—or permissions—needed to perform their job functions.

- ✓ **Establish Incident Response Plans**

  Develop and maintain a comprehensive incident response plan to ensure quick and effective action when a security breach is detected.

- ✓ **Use Anti-Phishing Technologies**

  Implement email filtering and web security solutions to detect and block phishing attempts before they reach employees.

Future Predictions

As we conclude our analysis of Web3 security failures in Q3 2024, it's clear that the industry has made significant progress in mitigating vulnerabilities and reducing the frequency of successful attacks. Despite a few high-profile incidents, this quarter saw the lowest number of exploit cases in the past three years, along with a decline in the total value of assets stolen.

However, vigilance and proactive security measures remain crucial. Access control attacks continue to be, and likely will remain, the most damaging type of exploit, accounting for a disproportionate share of stolen funds.

On a positive note, we expect the amount of funds returned or frozen to remain high, even as the overall number of attacks decreases. There are now more tools available to facilitate this, along with better capabilities to notify exchanges where stolen funds could be laundered, and a regular practice of rewarding white hat hackers after the recovery of funds.

Looking ahead, we anticipate a decrease in both the frequency and scale of bridge hacks, thanks to the adoption of newer, more secure architectures. Nonetheless, it is essential for projects to prioritize comprehensive security audits, maintain active bug bounty programs, and implement automated incident response strategies to further mitigate risks.

As the Web3 industry continues to evolve, collaboration, knowledge sharing, and a proactive approach to security will be key to building a more resilient and trustworthy ecosystem. By learning from past incidents and adopting best practices, we can pave the way for a future where the benefits of decentralized technologies are realized without compromising the safety of users' assets.