CYVERS

2025

Annual trends in

security, fraud, scams, risk management, and compliance.

Table of Contents

Overview

2025 marks an inflection point for crypto security and fraud. On one side, Cyvers' threat intelligence shows record losses from on chain attacks, driven primarily by large scale access control breaches. On the other hand, our fraud analytics reveal that industrialized social engineering operations, especially authorized fraud (like pig butchering schemes), have reached an unprecedented scale across exchanges, wallets, payment providers, and banking rails.

Cyvers observed over $2.5 billion in stolen funds in security incidents, up from $2.36 billion in 2024 and $1.69 billion in 2023. Access control attacks were the clear driver, causing over $2.2 billion in losses, while smart contract and code vulnerabilities dropped to about $292 million. Across 108 incidents, a handful of very large access control breaches in Q1 generated most of the financial damage, with Ethereum remaining the primary target and a long tail of other chains still seeing high impact single events.

At the same time, crypto fraud has matured into an industrial enterprise. In 2025 Cyvers detected almost $16 billion in fraudulent activity value across over 4.3 million transactions, 780,000 fraudulent addresses, and at almost 19,000 fraud networks active on more than 140 exchanges and venues. Authorized fraud, especially pig butchering schemes, dominated this landscape, using social engineering and fake investment platforms to push victims into approving their own losses. Activity was heavily concentrated in a few liquid assets, mainly USDT, ETH, and USDC, and in a small set of systemically important exchanges and a large stablecoin issuer.

Against this backdrop, Cyvers' preemptive monitoring proved critical. Our systems exclusively detected over $2 billion in stolen value across 52 high-impact attacks. These results show that real-time analytics can meaningfully reduce losses on the chains, assets, and venues where fraud and security incidents are most concentrated and point the way toward a more proactive defense posture for the industry in 2025 and beyond.

About Cyvers

Cyvers is a leader in preventing threats and mitigating the risk of malicious activity in Web3. The company employs geometric machine learning and AI driven, graph based anomaly detection to analyze blockchain activity, surface emerging fraud and security patterns, and identify malicious behaviors before they fully materialize.

Cyvers serves a broad range of clients, including centralized exchanges, custodians, DeFi protocols, institutional trading platforms, payment service providers, and banks. By combining preemptive threat detection for access control and smart contract exploits with deep analytics on authorized and

unauthorized fraud, Cyvers helps its customers protect assets, strengthen compliance programs, and reduce their share of the more than $15 billion fraud problem that defined crypto in 2025.

Executive Summary

Overview.

In 2025 Cyvers observed a sharp escalation in both on-chain security incidents and crypto fraud. Direct hacks and exploits resulted in more than $2.5 billion in stolen funds, up from $2.36 billion in 2024.

Access control failures were the dominant driver, with over $2.2 billion lost to compromised keys, wallets, infrastructure, and privileged accounts, while smart contract and code vulnerabilities accounted for about $292 million.

Across 108 major incidents, access control made up less than half of cases by count, yet produced almost nine times the financial damage of code exploits.

Ethereum remained the primary battlefield, responsible for nearly 70% of value lost across 33 large incidents, while a long tail of ecosystems, including Sui, BNB Chain, and Bitcoin, continued to see high impact single events.

Crypto fraud - the biggest driver for losses - reached industrial scale. Cyvers's platform detected more than $15 billion in fraudulent value across over 4.2 million fraudulent transactions, more than 780,000 fraudulent addresses, and close to 19,000 active fraud networks transacting on more than 140 exchanges and trading venues.

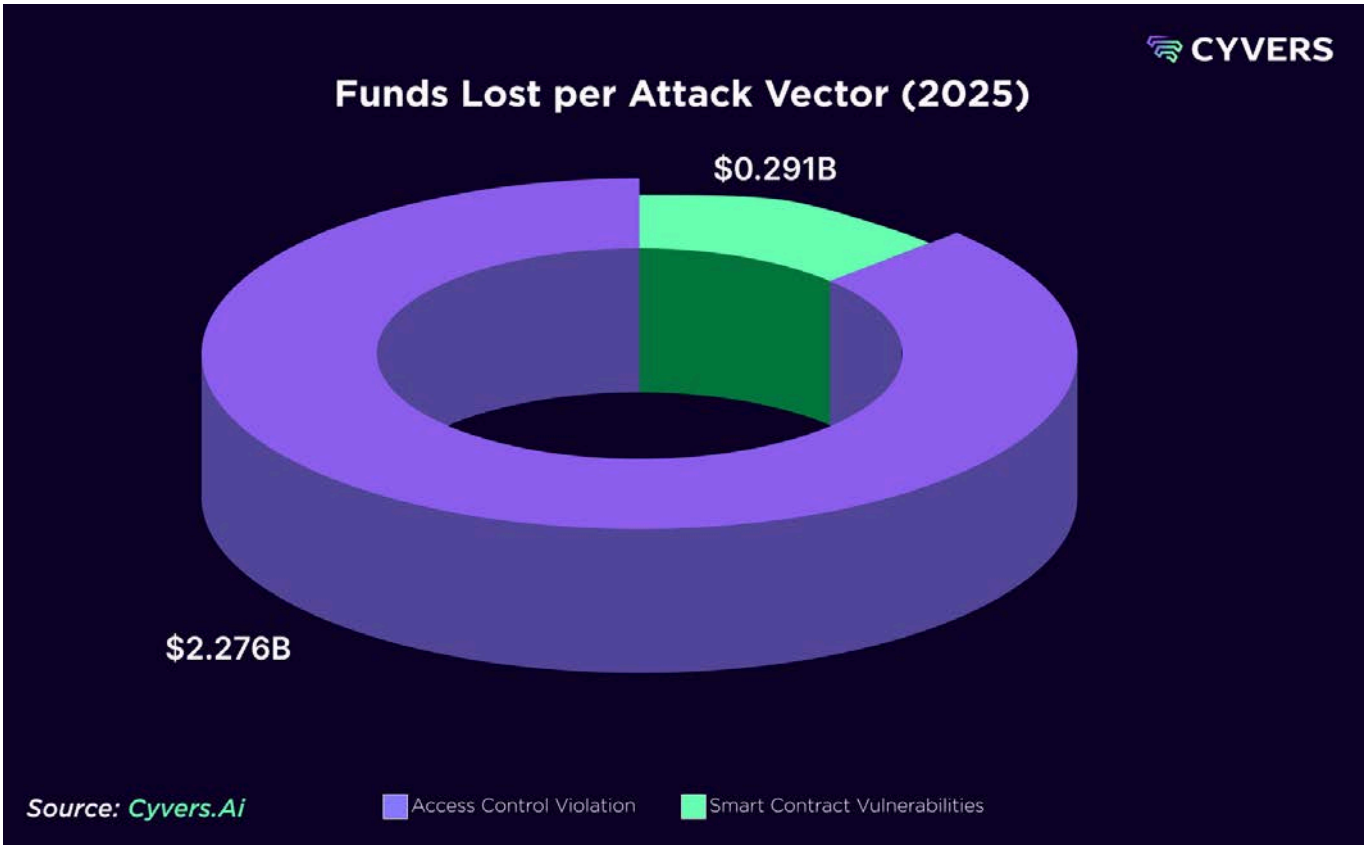
Authorized fraud, particularly pig butchering schemes, emerged as the most organized and persistent threat, using long term social engineering and fake investment platforms to push victims into approving their own losses.

Fraudulent flows were heavily concentrated in a small set of liquid assets, mainly USDT, ETH, and USDC, and in a handful of systemically important exchanges, which together carried the majority of detected fraud volume.

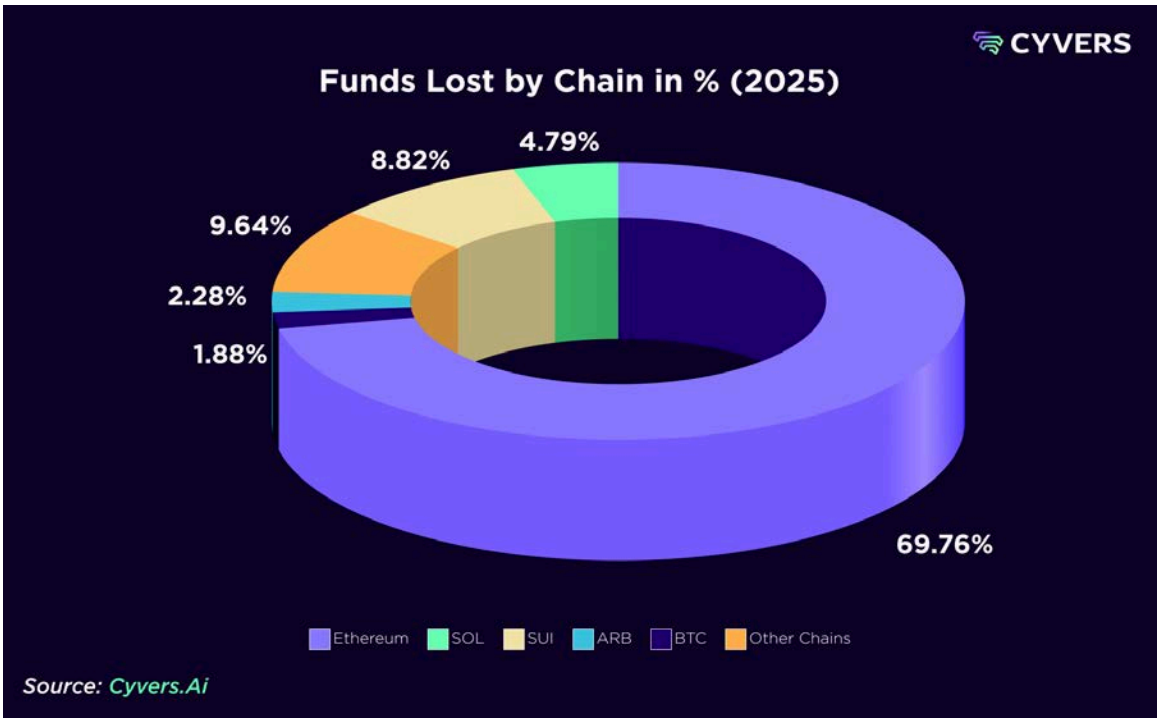
Key Stats of Malicious Activity. Annual and structural patterns.

Total on-chain losses from hacks and exploits in 2025 exceeded $2.5 billion, compared with $2.36 billion in 2024 and $1.69 billion in 2023.

Access control breaches accounted for more than 88% of hacked value in 2025, while code vulnerabilities represented about 11%. Cyvers recorded 51 access control incidents and 57 code vulnerability incidents.



By chain, Ethereum accounted for roughly 69.76% of all stolen funds and 33 major incidents. BNB Chain, Bitcoin, Arbitrum, Base, Sui, and other ecosystems together made up the remaining share, often through fewer but still significant incidents.

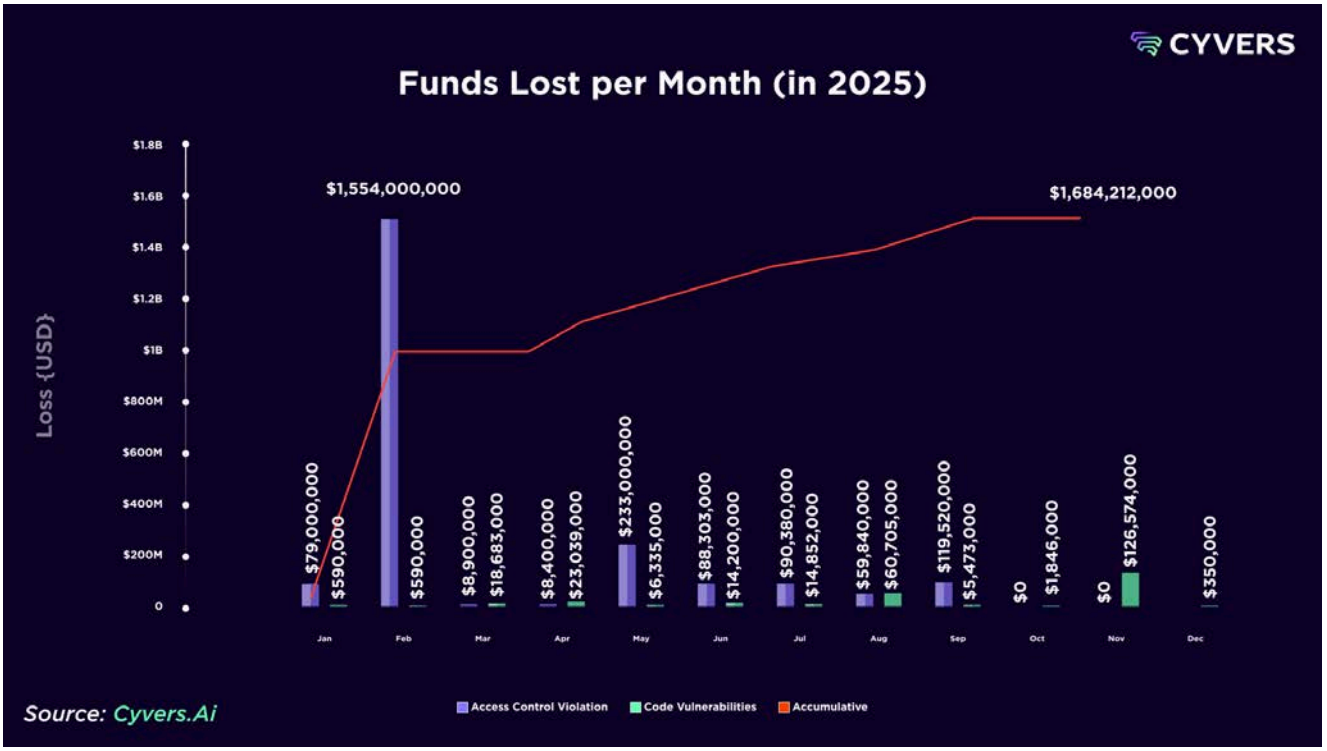


Quarterly and monthly highlights.

Q1 2025 was the most damaging quarter, with about $1.68 billion stolen, nearly two-thirds of the annual hacked value, despite recording fewer incidents than Q2 and Q3. Q2 and Q3 each saw losses in the mid 300 million range, while Q4 dropped to around 164 million dollars.

Incident activity peaked in Q2 with 37 cases, followed by 30 in Q3. Q4 was the quietest period by count, with only 11 incidents.

February stood out as the single worst month by value, with roughly $1.57 billion lost, driven by several large access control breaches. May was the second most damaging month at about $247 million, while April and December recorded the lowest losses.

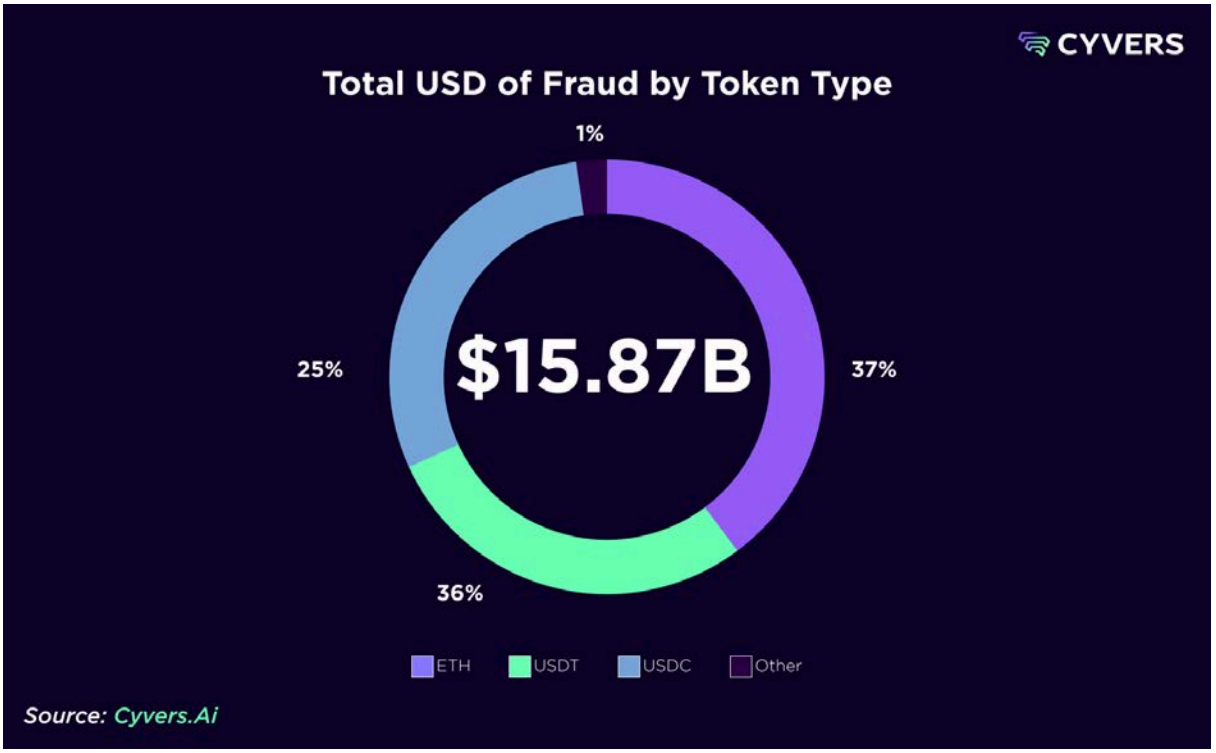


Fraud landscape metrics.

More than $15 billion in fraudulent value was detected in 2025, across over 4.2 million fraudulent transactions and more than 780,000 fraudulent addresses.

Fraud volumes climbed from roughly $1.2 billion in January to a peak of close to $1.6 billion in August, with September crossing about $1.2 billion before a decline in the final quarter.

USDT, ETH, and USDC together carried virtually the entire fraud volume, while all other tokens combined contributed only a small fraction, reflecting the strong preference of fraud networks for deep liquidity and fast fiat off-ramps.



Notable Incidents

2025 was defined by a small number of very large breaches that reshaped the risk profile for exchanges, protocols, and infrastructure providers.

- The Bybit exploit in February was the largest crypto theft on record, with attackers abusing a supply chain and access control vulnerability in a Safe-based wallet setup to divert about $1.5 billion. Cyvers was first to detect the anomalous outflows and trace the attack path.
- A catastrophic Cetus DEX exploit on Sui drained approximately $220 million by abusing fake token pools and liquidity manipulation, highlighting composability and token validation risks in newer ecosystems.
- The Balancer V2 ComposableStablePool exploit in November led to about $120 to $129 million in losses through precision-loss arithmetic and price manipulation across multiple networks.
- Additional high impact events included the Nobitex hot wallet compromise at around $90 million, the Phemex hot wallet breach at roughly $74 million, and multi-chain access control incidents at BtcTurk, CoinDCX, GMX, UXLINK, SwissBorg, UPCX, BitoPro, WOO X, and others.

- On the fraud side, Cyvers observed the largest single fraud transfer of the year at over 30.6 million dollars in ETH on a leading centralized exchange, alongside extensive pig butchering and authorized fraud networks moving billions through stablecoin rails.

These incidents underscore that access control, insider abuse, supply chain compromise, and DeFi logic flaws can each trigger systemic scale losses when not mitigated by runtime controls and continuous monitoring.

Cyvers's Innovative Solutions

In response to this threat landscape, Cyvers expanded its product suite in 2025 to deliver preemptive protection across security, fraud, and compliance functions.

- **Secure Co-Signing for Wallets:** an intelligent co-signer that simulates every transaction before approval, evaluates balance changes and contract state diffs, enforces policy rules, and blocks high risk operations such as malicious upgrades, treasury drains, or blind signing events. This control directly addresses the class of failures seen in incidents like Bybit and other access control breaches.
- **Cyvers Agents:** generative AI copilots that sit on top of Cyvers' real time intelligence graph, allowing security, fraud, and compliance teams to query wallets, entities, and transactions in natural language, reconstruct complex attack paths, and produce audit ready narratives for investigations.
- **The Stablecoin Trust Layer:** an integrated monitoring and risk platform for stablecoin issuers, custodians, exchanges, and payment companies, providing live mint and treasury surveillance, multi hop AML screening, fraud detection, and exploit alerts across chains where stablecoins serve as critical payment and settlement rails.
- **Liquidity Security for Trading Operations:** continuous monitoring and policy gating for trading firms, market makers, and liquidity providers, combining pre trade address and contract screening, validator and hot wallet anomaly detection, and automatic enforcement of routing and exposure limits when counterparties or venues show elevated risk.

Across hacks and fraud, Cyvers' exclusive detection metrics demonstrate the impact of these capabilities. In 2025 the platform exclusively detected approximately 2.12 billion dollars in stolen value across 52 high impact incidents, including about 1.89 billion dollars from access control breaches and 228 million dollars from code vulnerability exploits.

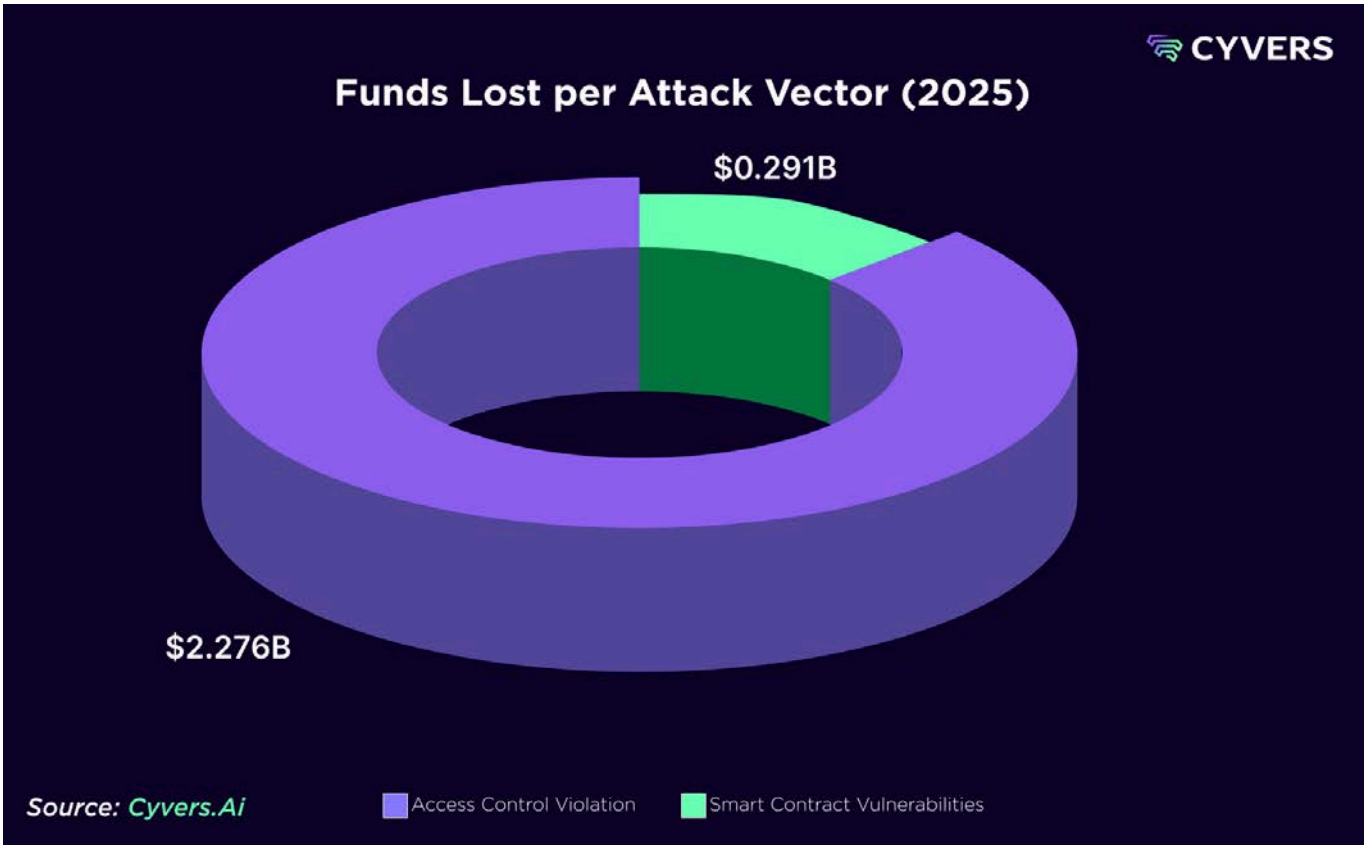

CYVERS
The Security Landscape in 2025

The Security Landscape in 2025

Types of incidents

Access control vs smart contract vulnerability attacks

In 2025, the Web3 threat landscape continued to tilt toward access control attacks, with losses from compromised keys, wallets, and centralized infrastructure reaching over 2.2 billion dollars. This represents an increase of almost 20% shift toward access control attacks, with losses from compromised keys, wallets, and centralized infrastructure exceeding $2.2 billion compared to 2024, when access control breaches accounted for about $1.9 billion in losses, and more than double the $1.08 billion recorded in 2023.

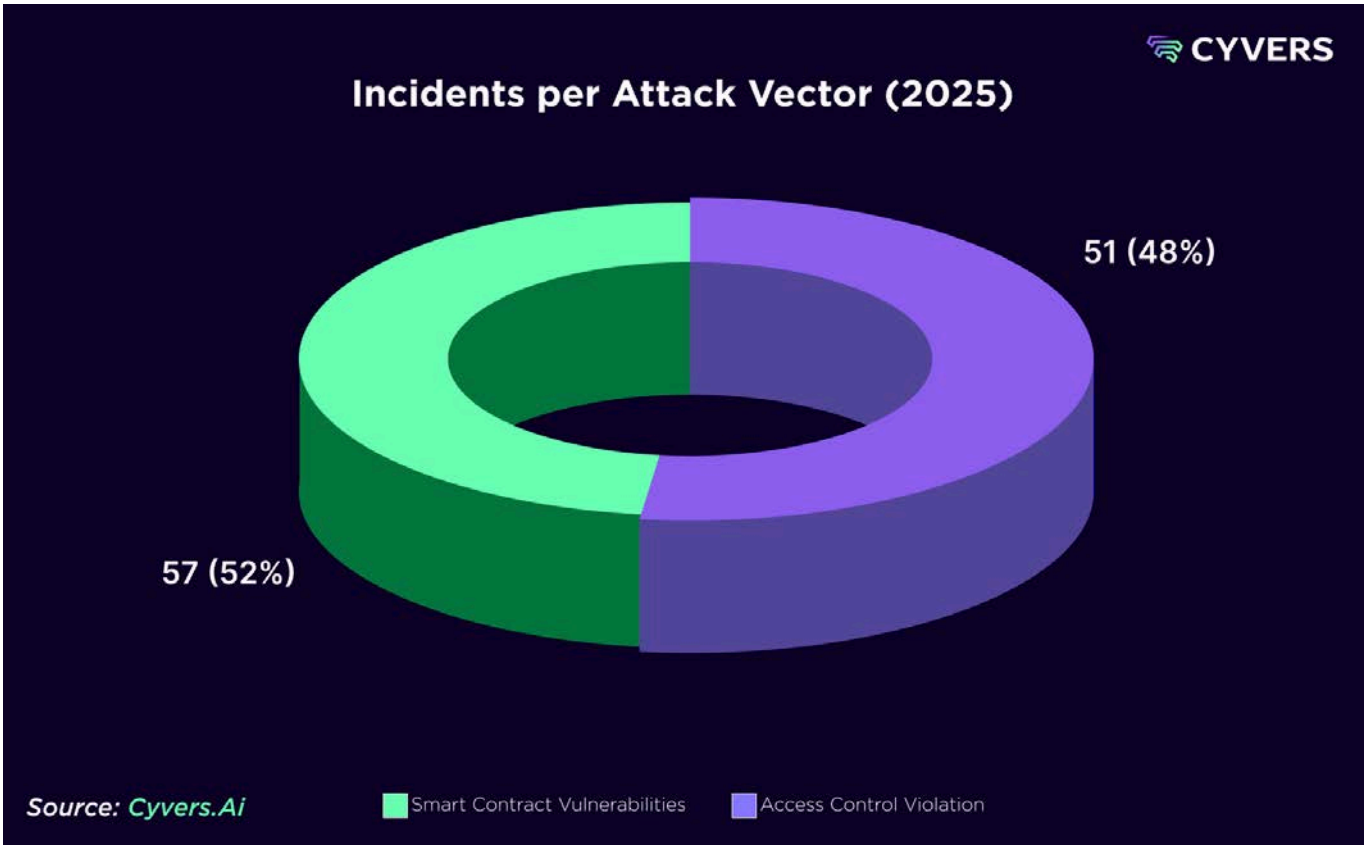


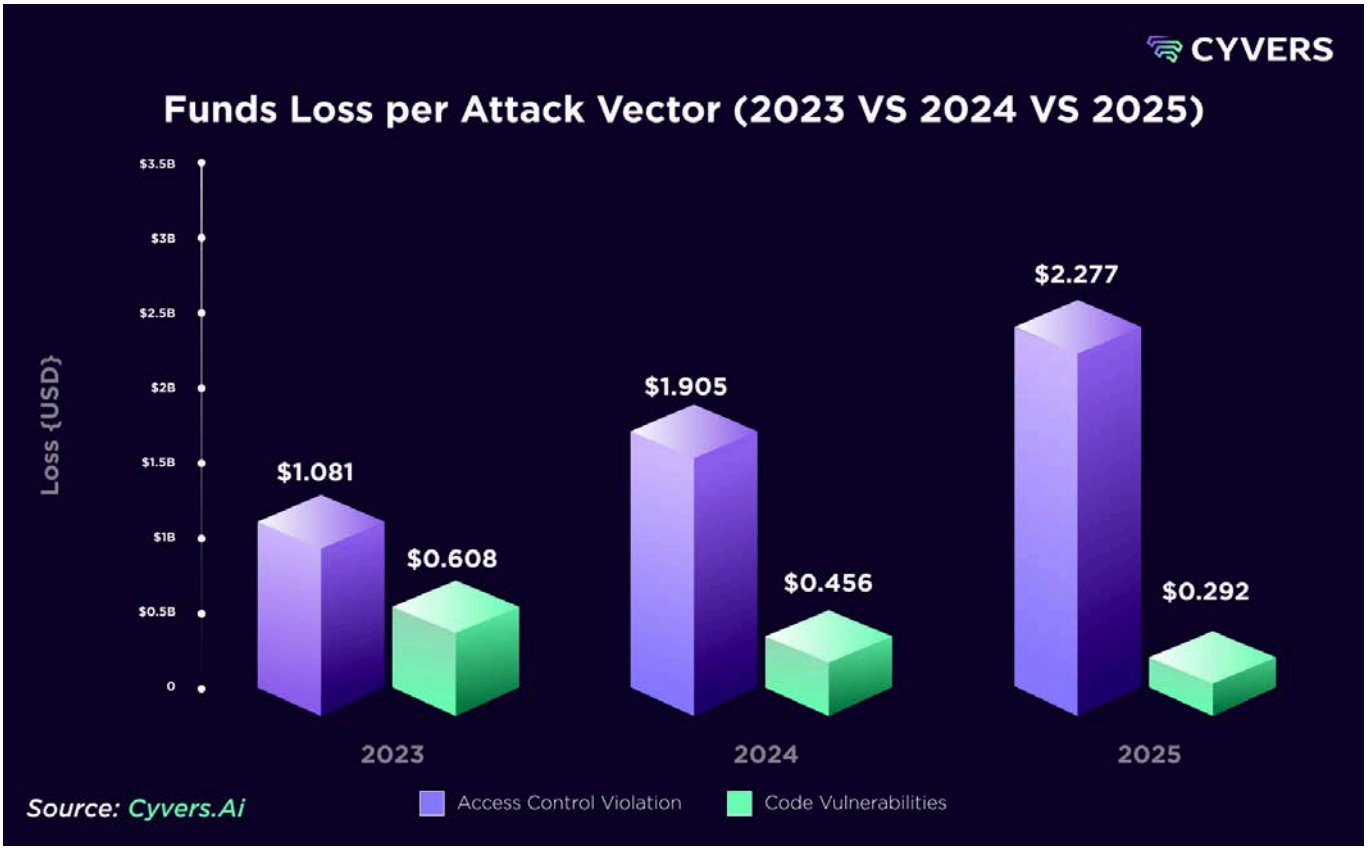
Smart contract and code vulnerability exploits moved in the opposite direction. Losses attributed to this vector fell to roughly $292 million, down about 36% from $456 million in 2024 and less than half the $608 million seen in 2023.

Across all vectors, total stolen value in 2025 climbed to over $2.5 billion, an increase of about 9% year over year, following the nearly 40% surge between 2023 and 2024. As a result, access control breaches dominated the financial impact: they were responsible for over 88.6% of all funds lost in 2025, while code vulnerabilities accounted for only 11.4%.

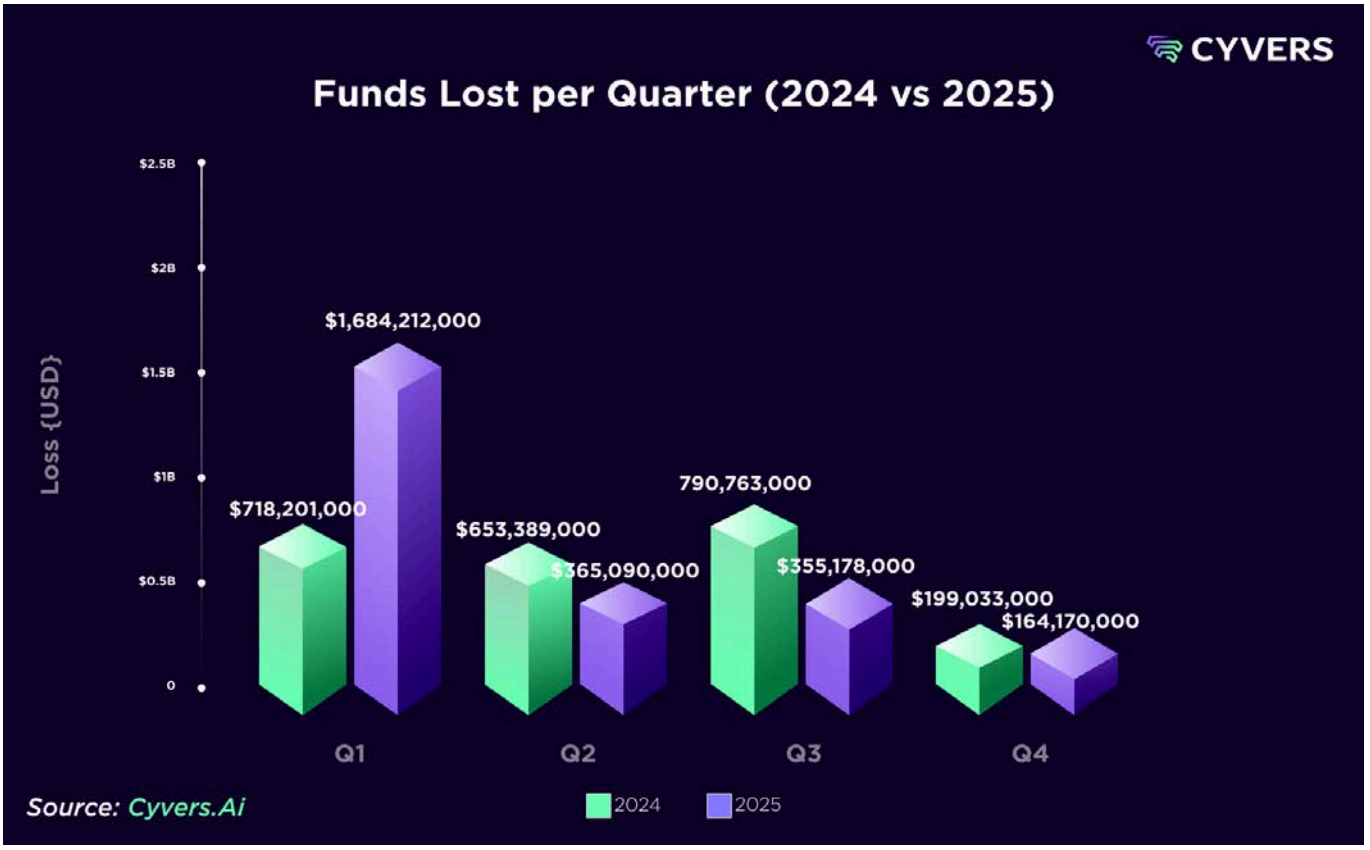
Incident counts tell a different story. Throughout 2025, Cyvers tracked 51 access control incidents and 57 smart contract vulnerability incidents, for a total of 108 attacks falling into these two categories. On average, an access control incident caused almost nine times more financial damage than a code vulnerability exploit. This gap highlights how a relatively small number of successful compromises of

centralized infrastructure or critical keys can overshadow dozens of smaller smart contract bugs in terms of value lost.





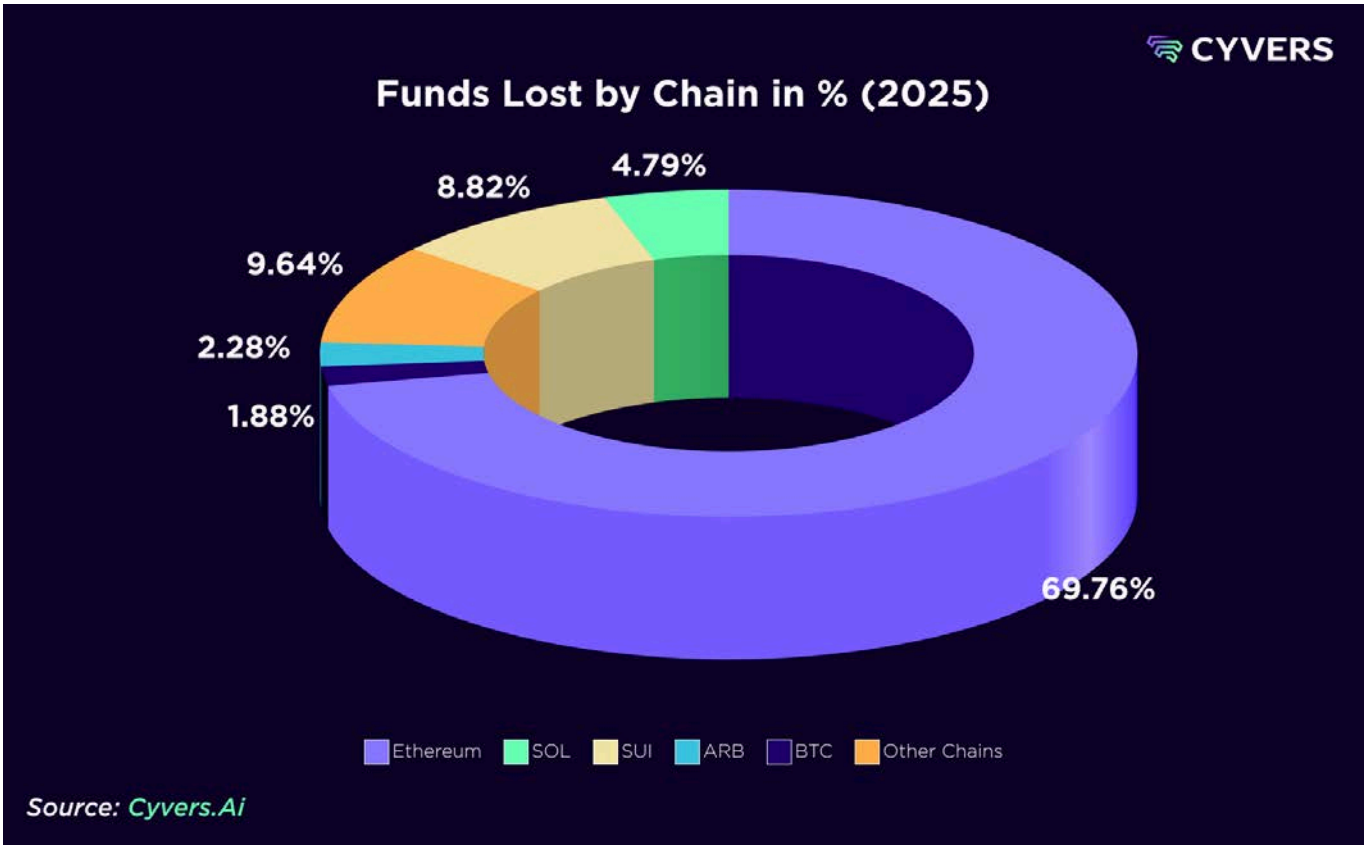
Quarterly patterns reinforce this picture. In terms of frequency, Q2 was the most active, with 16 access control and 21 code vulnerability incidents, followed by Q3 with 16 and 14 respectively. Q1 and Q4 were quieter by count, with 19 and 11 incidents. Yet Q1 was by far the most damaging quarter, as several very large access control breaches pushed losses to about $1.68 billion, or nearly two thirds of the year's total, even though it accounted for less than one fifth of all incidents.

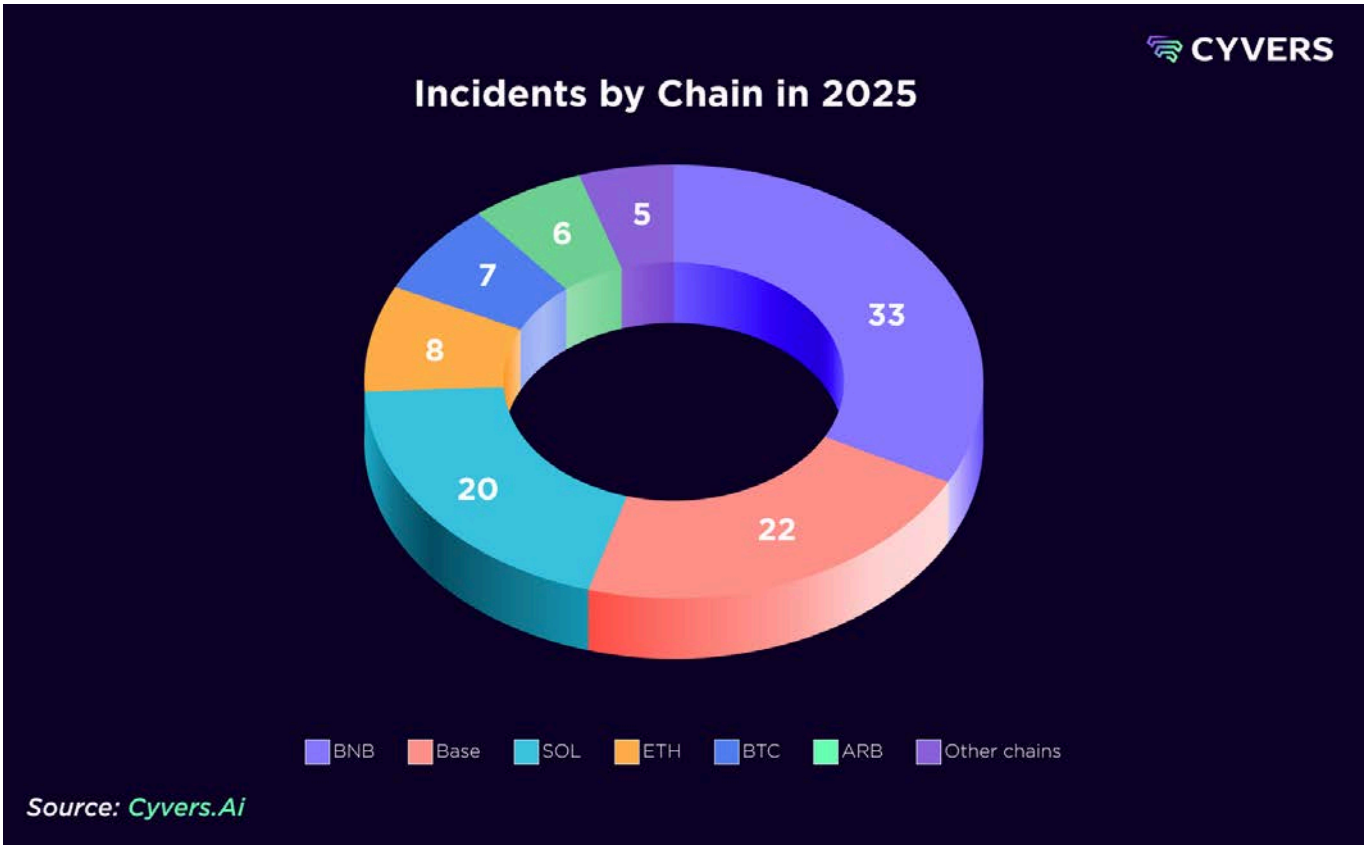


Attack breakdown by chain

The concentration of value on leading chains continued to shape attacker behavior in 2025.

- **Ethereum** remained the primary target, with 33 major incidents and approximately 69.76 percent of all funds lost. This confirms Ethereum as the chain where the highest value continues to be at risk, and where Cyvers' preemptive monitoring is most critical.
- **BNB Chain** experienced 20 incidents, but these accounted for only 2.5% of total value lost, indicating a high number of smaller sized attacks.
- **Other chains** collectively captured 9.64% of stolen funds across 22 incidents, underscoring the importance of coverage across the long tail of ecosystems.
- **Sui** stood out with 8.82% of total losses, despite not matching Ethereum's incident volume, which suggests that individual attacks on newer ecosystems can still be very high impact.
- **Bitcoin** saw five incidents and 1.88% of losses, while **Arbitrum and Base** accounted for 2.28% and 0.33% of total value respectively.





The distribution of incidents by chain confirms a dual reality: Ethereum remains the primary battlefield by value, yet the growing diversity of targeted chains requires monitoring capabilities that span both established and emerging ecosystems.

2025 Security Statistics

Annual overview

In 2025, total reported losses reached over $2.5 billion across all vectors, up from $2.36 billion in 2024, and $1.69 billion in 2023. The rise in 2025 was driven almost entirely by large access control incidents, while code vulnerabilities became less costly overall.

In conclusion, these insights provide a stark overview of the challenges faced within Web3 security and highlight the need for continued vigilance and advanced security solutions to protect against an ever-evolving array of threats.

Quarterly statistics

Number of incidents per quarter

Incident counts were unevenly distributed across the year.

- **Q1** recorded 7 access control and 12 code vulnerability incidents.
- **Q2** was the most active period with 37 incidents in total, split between 16 access control and 21 code vulnerabilities.
- **Q3** followed with 30 incidents, divided relatively evenly between the two vectors.
- **Q4** was the quietest quarter, with only 3 access control and 8 code vulnerability incidents.

Funds lost per quarter

The financial impact did not follow the same pattern.

- **Q1** 2025 was the most damaging quarter by far, with about $1.68 billion stolen. This is more than 2.3 times the losses recorded in Q1 2024 and accounts for roughly 65% of all 2025 funds lost.
- **Q2 and Q3** recorded similar loss levels at around $365 million and $355 million, respectively, both significantly lower than in 2024, when these quarters each exceeded $650 million and $790 million.
- **Q4** was the least costly quarter in 2025, with about $164 million in losses, down from $199 million in Q4 2024.

This mismatch between incident counts and value reinforces a central theme: a single large scale access control breach can overshadow multiple smaller code exploits.

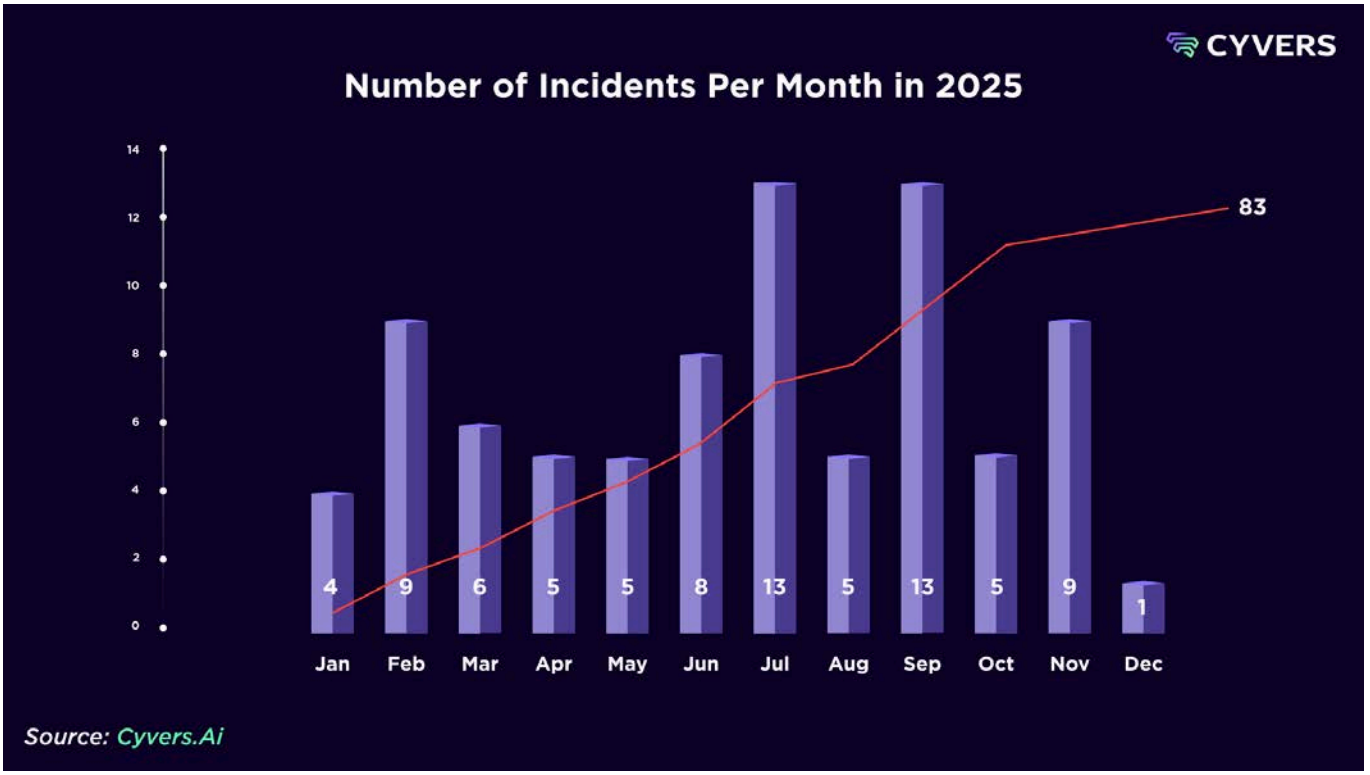
Monthly statistics

Number of incidents per month

Monthly activity in 2025 was highly uneven.

- July and September were the most active months, each with 13 incidents, followed by February and November with 9 incidents each.
- January, April, May, August, and October saw between 4 and 5 incidents, while December recorded only one incident, making it the quietest month of the year by count.

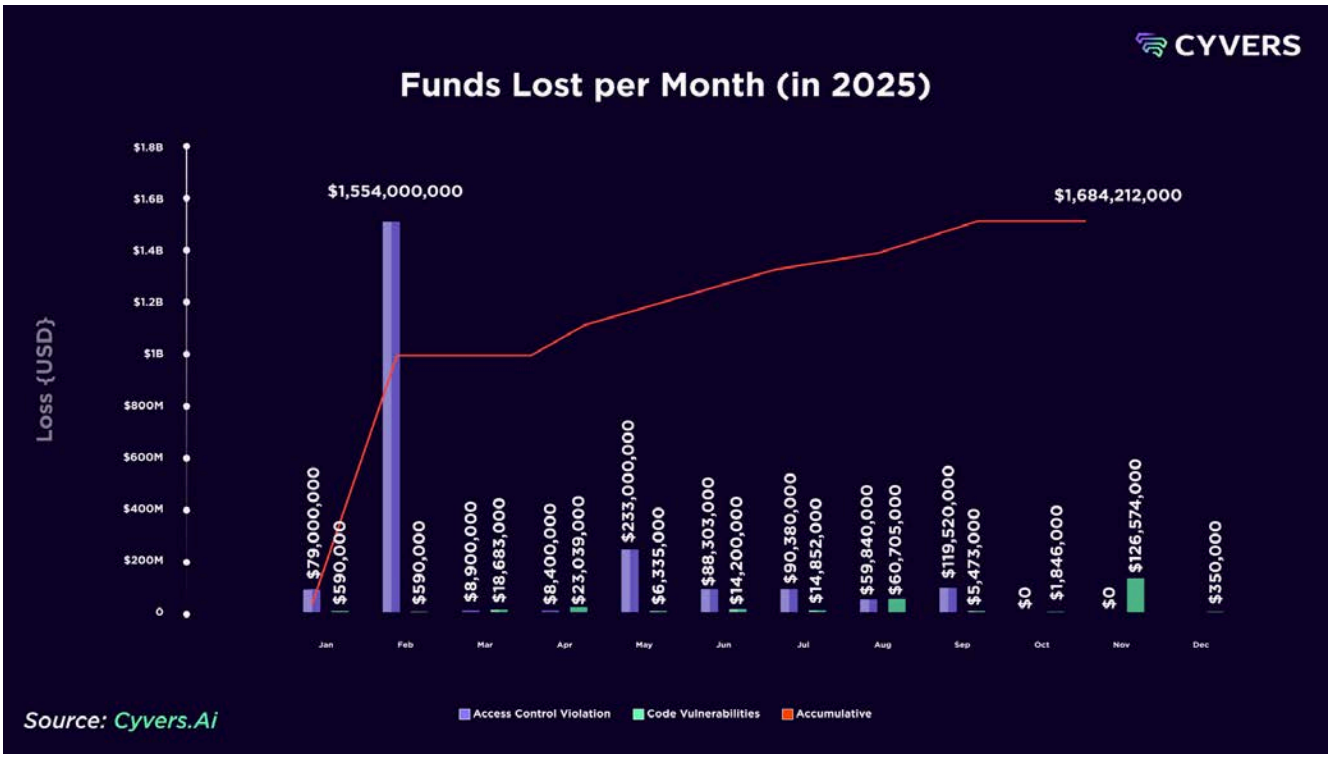
- Cumulatively, incident numbers built steadily through the first half of the year, reaching 37 by June and 82 by November before ending at 83 recorded incidents in the monthly view.



Funds lost per month

Financial losses followed a very different pattern.

- February was the most catastrophic month, with total losses of roughly $1.57 billion, driven almost entirely by massive access control breaches.
- May ranked second, with approximately $247 million lost across only five incidents, emphasizing again that severity does not depend solely on frequency.
- July and September each surpassed $130 million in losses, while June crossed the $100 million mark.
- April and December were comparatively mild, with around $14.7 million and $0.35 million in losses respectively.
- November was notable for code vulnerabilities, which generated about $126.6 million in losses in a month with no recorded access control losses.



Taken together, 2025 displayed pronounced spikes in both incident frequency and stolen value, yet these spikes often occurred in different months, underscoring the need for continuous monitoring rather than seasonal assumptions.

Cyvers exclusive detections in 2025

Cyvers' preemptive threat prevention platform played a leading role in identifying high impact incidents throughout 2025. The exclusively detected metrics capture cases where Cyvers was the only provider to flag the attack within this dataset.

- Across the year, Cyvers exclusively detected approximately $2.12 billion in stolen value, representing about 82% of the total losses covered in this report.
- This includes about $1.89 billion in access control breaches and $228 million in code vulnerability exploits, which correspond to roughly 83% of all access control losses and 78% of code vulnerability losses in 2025.

These results illustrate that while 2025 brought larger and more complex attacks, especially in the realm of access control, Cyvers consistently detected the most damaging incidents ahead of the broader market. This preemptive visibility was particularly vital on Ethereum and across high value access control breaches, where early detection can mark the difference between contained damage and systemic loss.

Top Incidents of 2025

2025 was a landmark year for security breaches in Web3, with multiple billion-dollar threats reshaping the industry's understanding of risk. Several incidents this year now rank among the largest crypto attacks in history, both in scale and sophistication. Cyvers was instrumental in uncovering, analyzing, and in many cases mitigating these threats, reinforcing the critical need for preemptive AI-powered solutions.

Prominent incidents and analysis

1st Quarter

Phemex Exchange Hack (January 23, 2025)

Company: Phemex Exchange
Amount Lost: $74 million
Attack vector: Access control violation

Incident Overview:
On January 23, 2025, Phemex, a Singapore-based cryptocurrency exchange, suffered a security breach resulting in the theft of approximately $74 million in assets. The incident involved multiple blockchains and included stablecoins such as Tether (USDT) and USD Coin (USDC), along with other tokens. The breach stemmed from an access control failure in the exchange's hot wallet infrastructure, enabling attackers to compromise wallet keys and authorize unauthorized transfers.

Cyvers' Role:
Cyvers' artificial intelligence system detected more than $74 million in suspicious crypto outflows from Phemex's hot wallets across multiple blockchains, including BNB, Polygon, Arbitrum, and Base. We identified about 125 suspicious transactions involving various tokens and stablecoins, some of which were already swapped to Ether to avoid freezing measures. Cyvers prompted Phemex to temporarily suspend withdrawals, carry out an emergency security inspection, and enhance its wallet monitoring and access controls.

Aftermath:
Following the breach, Phemex temporarily suspended withdrawals and initiated an internal investigation while collaborating with security and forensic experts. This breach emphasizes the need for robust access controls, effective key management, and continuous monitoring to secure hot wallet

infrastructure. The scale of the loss underscores the critical importance of proactive security measures for cryptocurrency exchanges to mitigate future risks.

Bybit Hack (February 21, 2025)

Company: ByBit Exchange
Amount Lost: $1.5 billion
Attack vector: supply-chain and access control attack - blind signing.

Incident Overview:
On February 21, 2025, Bybit, a Dubai-based cryptocurrency exchange, suffered a major security breach resulting in unauthorized transactions totaling approximately $1.5 billion. The stolen assets included USDT, stETH, mETH, cmETH, ETH, among others. The breach was executed through a sophisticated supply-chain and access control attack on Safe{Wallet}'s user interface, which manipulated transaction approvals and allowed attackers to gain control of Bybit's wallets.

Cyvers' Role:
Cyvers' artificial intelligence system was the first to detect multiple irregular transactions on February 21, 2025, flagging suspicious outflows that ultimately amounted to $1.5 billion in digital assets. Detailed analysis by Cyvers revealed that attackers had inserted malicious code into Safe's frontend, tricking Bybit signers into approving compromised transactions. Cyvers promptly reported these findings, enabling early awareness of the breach and underscoring the need for robust supply-chain security and continuous monitoring of wallet infrastructure.

Aftermath:
Following the breach, Bybit initially denied direct responsibility, attributing the incident to vulnerabilities in Safe's infrastructure. The exchange has since suspended certain operations while investigations continue. This breach highlights the importance of stringent supply-chain security, UI integrity checks, and proactive monitoring to safeguard digital assets. The scale and sophistication of the attack emphasize the urgent need for cryptocurrency exchanges to reassess and strengthen their security frameworks against advanced threat vectors.

zkLend Hack (February 12, 2025)

Company: zkLend Protocol
Amount Lost: $9.5 million
Attack vector: Smart contract exploit

Incident Overview:
On February 12, 2025, zkLend, a decentralized money-market protocol built on StarkNet, suffered a security breach that resulted in the theft of approximately $9.5 million. The attacker exploited a vulnerability in zkLend's lending contracts, enabling unauthorized withdrawals from its pools. The stolen assets, largely converted into Ether (ETH), were bridged from StarkNet to Ethereum, with attempts to launder funds through privacy protocols such as Railgun.

Cyvers' Role:
Cyvers' artificial intelligence system was the first to flag the abnormal transactions on February 12, identifying suspicious fund movements from zkLend to Ethereum. Further analysis revealed the attacker had exploited a flaw in contract logic to siphon funds and attempt laundering via Railgun. Cyvers promptly reported these findings, enabling rapid awareness of the incident and underscoring the importance of monitoring Layer-2 ecosystems for abnormal cross-chain activity.

Aftermath:
Following the breach, zkLend offered the attacker a 10% white-hat bounty if 90% of the funds were returned, but the deadline passed without cooperation. The team then paused operations, engaged with law enforcement, and began forensic investigations. This incident highlighted the critical need for robust auditing of StarkNet contracts and emphasized the risks of cross-chain laundering attempts, underscoring the necessity of real-time monitoring.

Infini Hack (February 24, 2025)

Company: Infini Stablecoin Neobank
Amount Lost: $49.5 million
Attack vector: Access control breach

Incident Overview:
On February 24, 2025, Infini, a Hong Kong-based stablecoin payment platform, experienced a catastrophic breach resulting in the theft of approximately $49.5 million in USD Coin (USDC). The incident was attributed to an insider or compromised developer account with administrative privileges, which enabled unauthorized withdrawals from Infini's treasury wallets.

Cyvers' Role:
Cyvers' artificial intelligence system detected the sudden mass outflows of USDC from Infini on February 24, flagging them as suspicious. Its analysis confirmed that the withdrawals stemmed from privileged access abuse rather than external contract exploitation. By surfacing these details early, Cyvers provided critical insight into the insider nature of the attack and the immediate laundering of funds across multiple blockchains.

Aftermath:
In response, Infini filed legal action against a former developer suspected of orchestrating the breach and communicated an on-chain injunction to freeze the attacker's wallets. The platform offered a 20% bounty for the return of stolen funds but received no cooperation, ultimately forcing it to suspend operations. This event underscored the dangers of insider threats and highlighted the importance of strict key management, timely access revocation, and the monitoring of privileged accounts.

Abracadabra.Money (March 25, 2025)

Company: Abracadabra.Money, a decentralized finance lending platform
Amount Lost: Approximately $13 million
Attack vector: Smart contract logic exploit

Incident Overview:
On March 25, 2025, Abracadabra.Money, a decentralized finance lending platform, experienced a security incident resulting in unauthorized transactions totaling approximately $13 million. The activity originated on Arbitrum (ARB) and interacted with **GMX and Spell contracts**, then the proceeds were bridged to Ethereum and distributed across multiple addresses. The assets involved included Ether (ETH) after bridging, with flows tied to Abracadabra's cauldrons that utilize GMX V2's GM pools. It was confirmed that GMX users were not affected, and the impact was isolated to Abracadabra/Spell cauldrons that relied on those pools.

Cyvers' Role:
Cyvers' artificial intelligence system exclusively detected multiple irregular transactions on March 25, 2025, flagging suspicious outflows on Arbitrum tied to GMX IO and MIM Spell contracts. Cyvers traced approximately $13 million that was bridged to Ethereum and distributed across a few addresses.

Further analysis by Cyvers confirmed that GMX users were not impacted, and that the incident was confined to Abracadabra/Spell's cauldrons integrated with GMX V2's GM pools. Cyvers promptly reported these findings, highlighting the need for rigorous integration reviews and continuous cross-chain monitoring.

Aftermath:
Following the breach, it was clarified that GMX users were unaffected, and the incident pertained to Abracadabra's cauldrons that rely on GMX V2 liquidity. This security event underscores the importance of stringent access controls, integration safeguards, and continuous monitoring across chains to protect pooled assets. The incident also highlights the necessity for protocols to reassess third-party dependencies, improve alerting on unusual bridge activity, and strengthen risk controls to prevent similar breaches.

2nd Quarter

UPCX Exploit (April 1, 2025)

Company: *UPCX, an open-source blockchain payment platform*
Amount Lost: $70 million
Attack vector: Access control failure

Incident Overview:
In April 2025, UPCX, an open-source blockchain payment platform, suffered a major exploit that resulted in losses of approximately $70 million in its native UPC tokens. The attacker compromised the platform's admin private key, upgraded a ProxyAdmin contract, and invoked a privileged "withdrawByAdmin" function to siphon funds.

Cyvers' Role:
Cyvers' AI-based monitoring system detected the unusual withdrawals from UPCX contracts, identifying the unauthorized admin upgrade and subsequent mass outflows. Cyvers quickly flagged the use of privileged functions, highlighting the root cause as an admin key compromise rather than a smart contract logic error.

Aftermath:
UPCX halted all transactions immediately and advised users to stop using old deposit addresses. The exploit underscored the importance of using multisignature governance and timelocks for admin privileges, as the reliance on a single key led to catastrophic losses. The project's token value dropped sharply, and recovery efforts focused on tracing stolen funds.

BitoPro Breach (May 8, 2025)

Company: *BitoPro, a Taiwan-based cryptocurrency exchange*
Amount Lost: Approximately $11.5 million
Attack vector: Hot wallet compromise, an access control failure across multiple chains enabling unauthorized withdrawals.

Incident Overview:
On May 8, 2025, BitoPro, a Taiwan-based cryptocurrency exchange, experienced a security breach that resulted in unauthorized transactions totaling approximately $11.5 million. The assets were drained from hot wallets across Ethereum, Tron, Solana, and Polygon, with portions routed to decentralized exchanges and later mixed through services such as Tornado Cash and THORChain. The assets involved included major stablecoins and tokens, for example Tether (USDT), USD Coin (USDC), and Ether (ETH). The breach was attributed to an access control failure in legacy hot-wallet infrastructure, which allowed attackers to execute unauthorized withdrawals.

Cyvers' Role:
Cyvers' artificial intelligence system detected multiple irregular transactions on May 8, 2025, enabling identification of multi-chain outflows from BitoPro's hot wallets and subsequent swaps on DEXs. Further analysis correlated the movements with laundering patterns, including stablecoin conversions and cross-chain routing, helping quantify losses near $11.5 million and highlight the need to harden hot-wallet operations and monitoring.

Aftermath:
Following the breach, BitoPro initially cited "maintenance," then confirmed the hack weeks later, stating that withdrawals remained available and that most funds were held in unaffected cold wallets. The exchange said it would compensate users and engaged external investigators, underscoring the importance of stringent access controls and continuous monitoring to safeguard digital assets. The delayed disclosure highlighted the necessity for organizations to reassess incident-response playbooks and strengthen transparency to prevent future breaches.

Coinbase Breach (May 11, 2025)

Company: *Coinbase, a U.S.-based cryptocurrency exchange.*
Amount Lost: $400 million
Attack vector: Insider-enabled breach via social engineering, where third-party support contractors were bribed or coerced to reset accounts and enable fraudulent withdrawals

Incident Overview:
In May 2025, Coinbase, one of the largest U.S.-based cryptocurrency exchanges, suffered a breach of its customer support systems, leading to estimated losses of up to $400 million. Attackers bribed or coerced third-party support contractors, gaining unauthorized access to user accounts and executing fraudulent withdrawals.

Cyvers' Role:
Cyvers' system detected irregular withdrawal patterns linked to multiple high-value Coinbase accounts, flagging the transactions as coordinated insider-enabled fraud. Its analysis helped confirm the use of compromised support accounts as the primary vector, allowing investigators to differentiate between infrastructure hacks and social engineering-driven account takeovers.

Aftermath:
Coinbase terminated its relationship with the compromised contractor firm and fully reimbursed affected users. The incident highlighted that even robust infrastructure is vulnerable to human factors, prompting Coinbase to bring more support in-house, tighten access controls, and enhance fraud detection systems.

Cetus DEX Exploit (May 23-25, 2025)

Company: *Cetus, a decentralized exchange (DEX) on the Sui blockchain*
Amount Lost: Approximately $220 million in pooled assets
Attack vector: Fake pools created to drain funds

Incident Overview:
Between May 23 and May 25, 2025, Cetus, a decentralized exchange on the Sui blockchain, suffered a catastrophic exploit resulting in the loss of approximately $220 million. Attackers deployed fake tokens with spoofed metadata and manipulated pool balances, enabling them to drain liquidity pools of legitimate assets.

Cyvers' Role:
Cyvers' AI detected the deployment of suspicious tokens and subsequent abnormal liquidity withdrawals on Sui. The system identified token forgery and pool manipulation as the exploit vector, allowing a rapid response and warning to exchanges.

Aftermath:
Cetus immediately paused operations and began a recovery and reimbursement plan with the Sui Foundation. The incident emphasized the risks of inadequate token validation in DEXs and accelerated security efforts across the Sui ecosystem to prevent similar attacks.

Nobitex Hack (June 18, 2025)

Company: Nobitex, Iran's largest cryptocurrency exchange
Amount Lost: $90 million
Attack vector: Hot wallet compromise via stolen keys

Incident Overview:
On June 18, 2025, Nobitex, Iran's largest cryptocurrency exchange, was hacked, with attackers stealing around $90 million in crypto assets. The hacktivist group Predatory Sparrow claimed responsibility, gaining access to hot wallet private keys and draining assets across Ethereum, Tron, and Bitcoin networks. Some stolen funds were deliberately burned as a political statement.

Cyvers' Role:
Cyvers detected the cross-chain mass outflows from Nobitex's wallets, flagging the transactions as coordinated hot wallet compromises rather than typical market activity. By tracing assets across chains and identifying burn addresses, Cyvers provided critical intelligence on the hacktivist motivations behind the attack.

Aftermath:
Nobitex immediately moved remaining funds into cold storage and worked with authorities to investigate. The politically motivated nature of the attack underscored the risk of hacktivist and nation-state cyber activity targeting regional exchanges.

3d Quarter

GMX IO exploit (July 9, 2025)

Company: GMX, a decentralized perpetuals exchange
Amount Lost: Approximately $40 million
Attack vector: Smart contract exploit via reentrancy, abusing the GLP pool's short position update logic

Incident Overview:
In July 2025, GMX's V1 platform was exploited for around $40 million after attackers used a reentrancy vulnerability in the GLP pools. By manipulating the executeDecreaseOrder function, the attacker tricked the system into mispricing collateral and drained funds from liquidity pools.

Cyvers' Role:
Cyvers' system detected abnormal transaction patterns in the GMX V1 contracts, identifying the exploit as a reentrancy attack. The detection provided timely intelligence for exchanges and liquidity providers, enabling defensive measures against further exploitation.

Aftermath:
GMX immediately paused V1 minting and offered a 10% white-hat bounty for fund return. The newer GMX V2 was unaffected, and the hack accelerated migration away from legacy contracts. The incident emphasized the need for retiring outdated DeFi protocols once vulnerabilities are known.

CoinDCX Hack – (July 19, 2025)

Company: *CoinDCX, India's largest cryptocurrency exchange.*
Amount Lost: $44 million
Attack vector: Hot wallet compromise, likely through an insider or phishing of an operational treasury account

Incident Overview:
On July 19, 2025, CoinDCX, India's largest cryptocurrency exchange, suffered a breach resulting in the theft of approximately $44 million. Attackers compromised an operational treasury wallet used for liquidity provisioning, enabling them to siphon off 4,443 ETH and 155,830 SOL. The stolen assets were bridged across Solana and Ethereum to obscure their trail.

Cyvers' Role:
Cyvers' AI-based monitoring system flagged the irregular outflows, identifying the anomalous bridging of assets between Solana and Ethereum. The system helped confirm that the compromise stemmed from an operational account, rather than customer wallets, ensuring early clarity and enabling rapid response.

Aftermath:
CoinDCX confirmed that no customer assets were impacted and covered the losses from its corporate reserves. The exchange reported the incident to India's CERT-In and law enforcement, while also launching a bounty program for asset recovery. This incident highlighted the risks of operational treasury wallets and the need for stricter multi-signature controls.

WooX Breach (July 24, 2025)

Company: *WOO X, a Taiwan-based cryptocurrency exchange*
Amount Lost: Approximately $14 million
Attack vector: Phishing of a team member, leading to misuse of internal tools and unauthorized withdrawals from a limited set of user accounts

Incident Overview:
On July 24, 2025, WOO X, a Taiwan-based cryptocurrency exchange, experienced a security breach resulting in unauthorized transactions totaling approximately $14 million. The assets involved included major coins and stablecoins, for example Bitcoin (BTC), Ether (ETH), and USDT from a limited set of high-value user accounts. The breach was attributed to phishing of a team member, which allowed misuse of internal tools and enabled attackers to execute unauthorized withdrawals.

Cyvers' Role:
Cyvers' artificial intelligence system exclusively detected multiple irregular transactions on July 24, 2025, enabling the identification of coordinated withdrawals across a small group of WOO X user accounts. Further analysis correlated account takeover behavior with insider-tool misuse and traced asset movements, including rapid swaps and attempted laundering, bringing the total amount stolen to roughly $14 million. Cyvers promptly reported these findings, highlighting the critical need for strong access controls, strict admin tooling protections, and continuous monitoring.

Aftermath:
Following the breach, WOO X temporarily paused withdrawals and initiated an internal investigation, while coordinating with exchanges and analytics partners to block further outflows. This security breach underscores the importance of implementing stringent access control measures and real-time monitoring to safeguard digital assets. The incident highlights the necessity for organizations to reassess and strengthen their anti-phishing training, admin-tool protections, and withdrawal verification protocols to prevent future breaches.

BtcTurk Hack (August 14, 2025)

Company: *BtcTurk, Turkey's leading cryptocurrency exchange*
Amount Lost: *$50 million*
Attack vector: *Hot wallet compromise across multiple blockchains*

Incident Overview:
On August 14, 2025, BtcTurk was hacked for about $50 million. Attackers accessed multiple hot wallet keys, draining assets across Ethereum, Tron, and Bitcoin networks. This was BtcTurk's second major hack in two years, raising concerns about persistent vulnerabilities.

Cyvers' Role:
Cyvers' AI flagged the unusual cross-chain outflows, identifying simultaneous withdrawals across different blockchains as a sign of hot wallet compromise. The system's multi-chain tracing provided immediate intelligence for exchanges to block potential laundering attempts.

Aftermath:
BtcTurk suspended withdrawals and moved remaining funds to cold storage. The exchange pledged to cover customer losses and began a full security overhaul. The repeat breach emphasized the importance of continuous penetration testing and defense-in-depth for exchanges.

SwissBorg Exploit (September 8, 2025)

Company: *SwissBorg, a Swiss crypto wealth management platform*
Amount Lost: *$41.5 million*
Attack vector: *Third-party API compromise via integration with a staking provider*

Incident Overview:
On September 8, 2025, SwissBorg suffered an exploit in its Solana Earn program, resulting in the theft of 192,600 SOL (~$41.5 million). Attackers exploited a vulnerability in API communications with third-party staking partner Kiln, enabling unauthorized withdrawals.

Cyvers' Role:
Cyvers' monitoring system detected the anomalous withdrawals from SwissBorg's Solana Earn wallets, attributing the exploit to third-party API abuse. Cyvers' insights helped frame the incident as a supply chain compromise rather than a direct protocol hack.

Aftermath:
SwissBorg suspended the Solana Earn program and pledged to fully reimburse affected users from treasury reserves. The company worked with the Solana Foundation and exchanges to freeze stolen funds. The breach underscored the risks of third-party dependencies and reinforced the importance of auditing external integrations.

UXLINK Breach (September 22, 2025)

Company: *UXLINK, a Web3 social and community platform*
Amount Lost: Approximately $48 million
Attack vector: Access control takeover

Incident Overview:
On September 22, 2025, UXLINK, a Web3 platform, experienced a security breach resulting in approximately $48 million in unauthorized transfers. An attacker executed a delegate call, removed the admin role, and invoked addOwnerWithThreshold to seize control, then transferred about $4 million USDT, $500,000 USDC, 3.7 WBTC, and 25 ETH. On Ethereum, USDT and USDC were swapped to DAI; on Arbitrum, USDT was swapped to ETH and bridged to Ethereum. The hacker minted more than 2 billion UXLINK tokens, roughly $11.3 million.

Cyvers' Role:
Cyvers' artificial intelligence system exclusively detected multiple irregular transactions on September 22, 2025, correlating the delegatecall, admin removal, and addOwnerWithThreshold sequence with rapid multi-chain fund movements. Cyvers traced stablecoin swaps to DAI on Ethereum, identified USDT to ETH swaps on Arbitrum followed by bridging to Ethereum, and monitored the 10 million UXLINK inflow to the secondary address, including the portion still unswapped. Cyvers promptly reported these findings, highlighting a privileged access takeover as the attack vector and enabling rapid awareness across exchanges and partners.

Aftermath:
Following the breach, UXLINK began an investigation, rotated privileged keys, and moved to secure affected wallets and permissions. The incident underscores the need for strict role-based access controls, multisignature thresholds for ownership changes, delegatecall minimization or sandboxing, and continuous cross-chain monitoring. Organizations should reassess governance controls, implement timelocks and alerting on admin changes, and harden incident response to prevent similar compromises.

SBI Crypto Breach (September 24, 2025)

Company: *SBI Crypto, a Bitcoin mining pool operator and subsidiary of Japan's SBI Group*
Amount Lost: Approximately $21 million
Attack vector: Hot wallet compromise, with funds moved through several instant exchangers and laundered via Tornado Cash, reportedly consistent with DPRK-linked tactics

Incident Overview:
On September 24, 2025, SBI Crypto, a Bitcoin mining pool operator and subsidiary of Japan's SBI Group, experienced a security breach that resulted in unauthorized transfers totaling approximately $21 million. Stolen assets included BTC, ETH, LTC, DOGE, and BCH, which were routed through several instant exchangers, then laundered via Tornado Cash. Investigators noted indicators consistent with DPRK, Lazarus Group tactics.

Cyvers' Role:
Cyvers' artificial intelligence system exclusively detected multiple irregular transactions on September 24, 2025, correlating outflows from wallets associated with SBI Crypto, the quick use of instant exchangers, and subsequent deposits into Tornado Cash. Cyvers' analysis mapped the multi-asset movements across chains, quantified losses near $21 million, and highlighted behavioral patterns aligned with known Lazarus laundering playbooks, enabling rapid awareness across exchanges and partners.

Aftermath:
As of early October 2025, public reports indicated that SBI Crypto had not yet issued a detailed public statement on the root cause, while third-party investigators attributed the incident to a hot wallet compromise and traced laundering through Tornado Cash. The breach underscores the importance of hardening hot wallet key management, enforcing strict withdrawal controls, and monitoring for rapid, multi-hop laundering patterns. It also highlights the need for proactive collaboration between mining pools, exchanges, and analytics firms to accelerate freezing and recovery.

4th Quarter

Balancer Breach (November 3, 2025)

Company: *Balancer, a decentralized finance protocol and automated portfolio manager and exchange*
Amount Lost: Approximately $120-129 million
Attack vector: Smart contract logic exploit in V2 ComposableStablePool math that caused precision loss and price manipulation via crafted batch swaps, enabling rapid liquidity drainage across multiple networks

Incident Overview:
On November 3, 2025, Balancer, a decentralized finance protocol, experienced a major exploit that drained roughly $120–$129 million from V2 pools across several networks. Investigations indicate the attacker abused a rounding and precision loss flaw in ComposableStablePool math, likely tied to the upscaleArray path, chaining crafted batchSwap calls to depress BPT pricing and extract value at scale. Stolen assets included liquid staking and ETH-based tokens such as WETH, wstETH, and osETH, and the draining was completed within minutes. Balancer advised users to stop interacting with affected V2 pools while the team and partners triaged the issue.

Cyvers' Role:
Cyvers' artificial intelligence system exclusively detected coordinated abnormal swaps and rapid liquidity extraction on November 3, 2025, correlating repeated batchSwap patterns with price distortions in Balancer's stable pools. Cyvers flagged the cross-chain outflows in near real time, helped attribute the vector to precision-loss arithmetic in V2 pool logic rather than a key compromise, and provided exchange partners with indicators to track and block laundering routes.

Aftermath:
Balancer and ecosystem partners paused or isolated impacted pools, issued user advisories, and began forensic review of V2 stable-pool math while encouraging migration to unaffected configurations. External researchers published timelines and technical breakdowns, and coverage estimated losses near $128 million. The incident reinforced the need for rigorous invariant testing, bounded arithmetic, and live anomaly detection for composable DEXs.

CYVERS

Crypto Fraud Landscape 2025

Crypto Fraud Landscape 2025

Authorized Crypto Fraud

Fraud in crypto is not a single phenomenon, but a spectrum of schemes that often overlap. The same fraud network can combine romance fraud, fake investments, phishing, and money mule activity in one operation.

In this article, we will focus on **authorized fraud**: situations where victims approve the transaction themselves, but only because they have been misled or manipulated. In these cases the wallet, exchange, or banking rails usually work exactly as intended. The problem is that the person behind the keyboard is acting under false beliefs.

Authorized fraud contrasts with unauthorized fraud, where attackers move funds without the victim's consent, for example, through account takeovers, SIM swaps, or malware. Because authorized transactions are technically "legitimate" and often considered final, they are harder to reverse and, in many jurisdictions, fall into a gray area for compensation and liability.

Within the broader universe of authorized fraud, this article will pay particular attention to **pig butchering.** This scheme has become the dominant form of authorized fraud in crypto, responsible for well over sixty percent of known authorized fraud volumes. It blends long term emotional grooming, fake investment platforms, and Ponzi like payout patterns into one highly efficient scam model.

By early 2025, crypto markets had fully emerged from the long winter that ended in mid 2023. The approval of multiple crypto ETFs and a strongly pro-crypto agenda in Washington fueled a surge of new retail and institutional inflows. That same wave of optimism attracted a parallel influx of criminal actors. Industry analysts now describe crypto fraud as an industrial scale activity, comparable in size to the illicit drug trade, with tens of billions of dollars in annual losses and hundreds of thousands of people involved, many of them operating from large scam compounds in Southeast Asia.

Previous Cyvers research into authorized fraud activity across 150 leading platforms in 2024, including centralized exchanges, PSPs, on and off ramps, and banks, already showed the scale of the problem. We identified over 200,000 cases involving more than 1.15 million fraudulent transactions and roughly 5.5 billion dollars in stolen funds. That dataset revealed that three of the five largest global exchanges by volume, a major crypto-friendly bank, and an institutional trading venue were among the most heavily impacted.

Fraud networks have adapted quickly to the transparency of blockchains. They split flows into many small payments, move assets through long chains of wallets, swap between tokens through DeFi protocols, and bridge across multiple chains. Fiat off-ramps include OTC brokers with weak KYC, money mules who cash out at exchanges, and conversion into prepaid or gift card instruments. Stablecoins, especially highly liquid dollar-pegged assets, play a central role because they allow scammers to move value quickly and exit into fiat with minimal price risk.

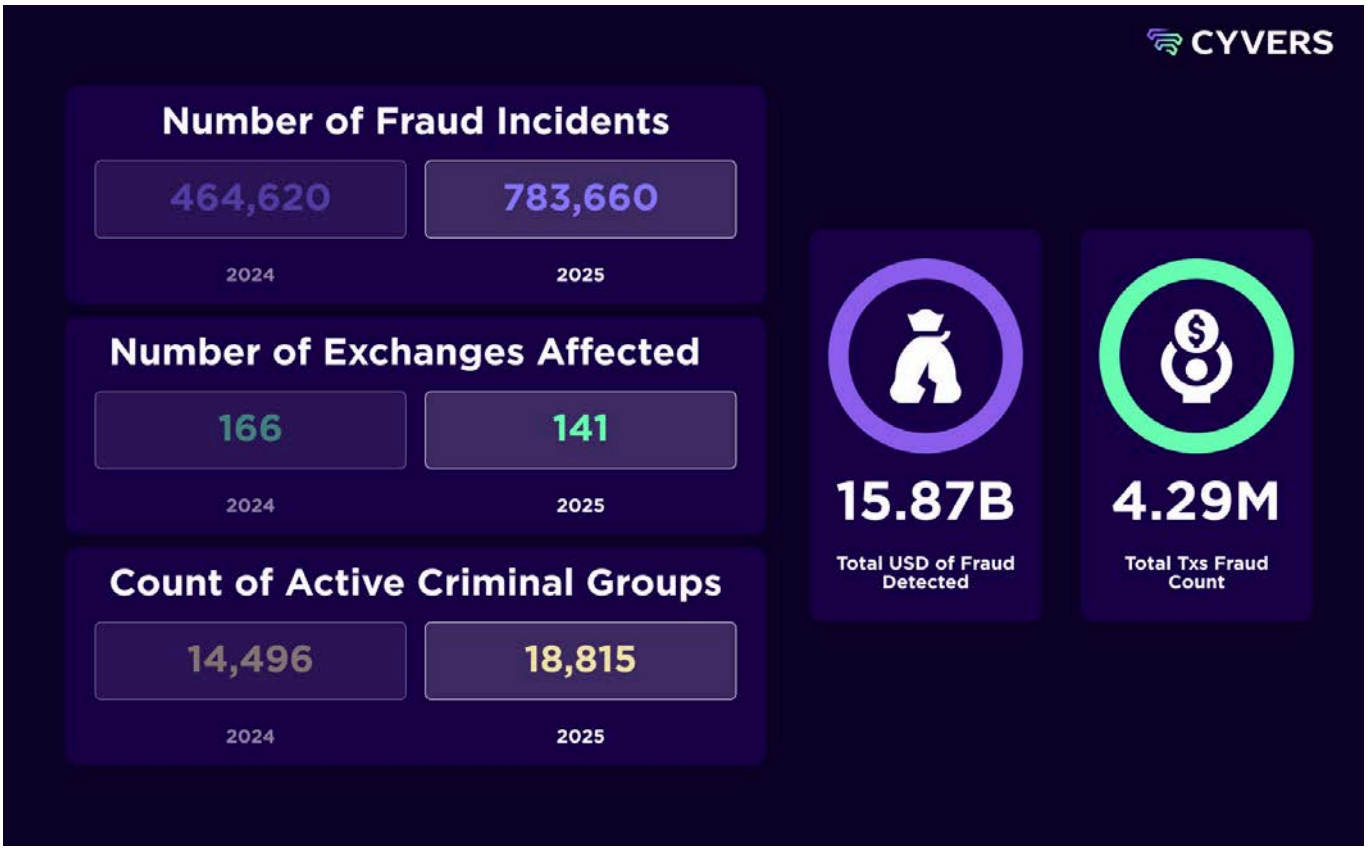
Against this backdrop, 2025 marks a turning point, with Cyvers data revealing record fraud volumes, unprecedented criminal coordination, and growing concentration of risk across major platforms.

2025 Overview

In 2025 Cyvers's preemptive threat prevention platform observed a sharp escalation in crypto fraud across exchanges, wallets, and payment rails. Over the year our systems detected:

- **More than 15 billion dollars in fraudulent value**
- **Over 4.2 million fraudulent transactions**
- **Over 780,000 fraudulent addresses**

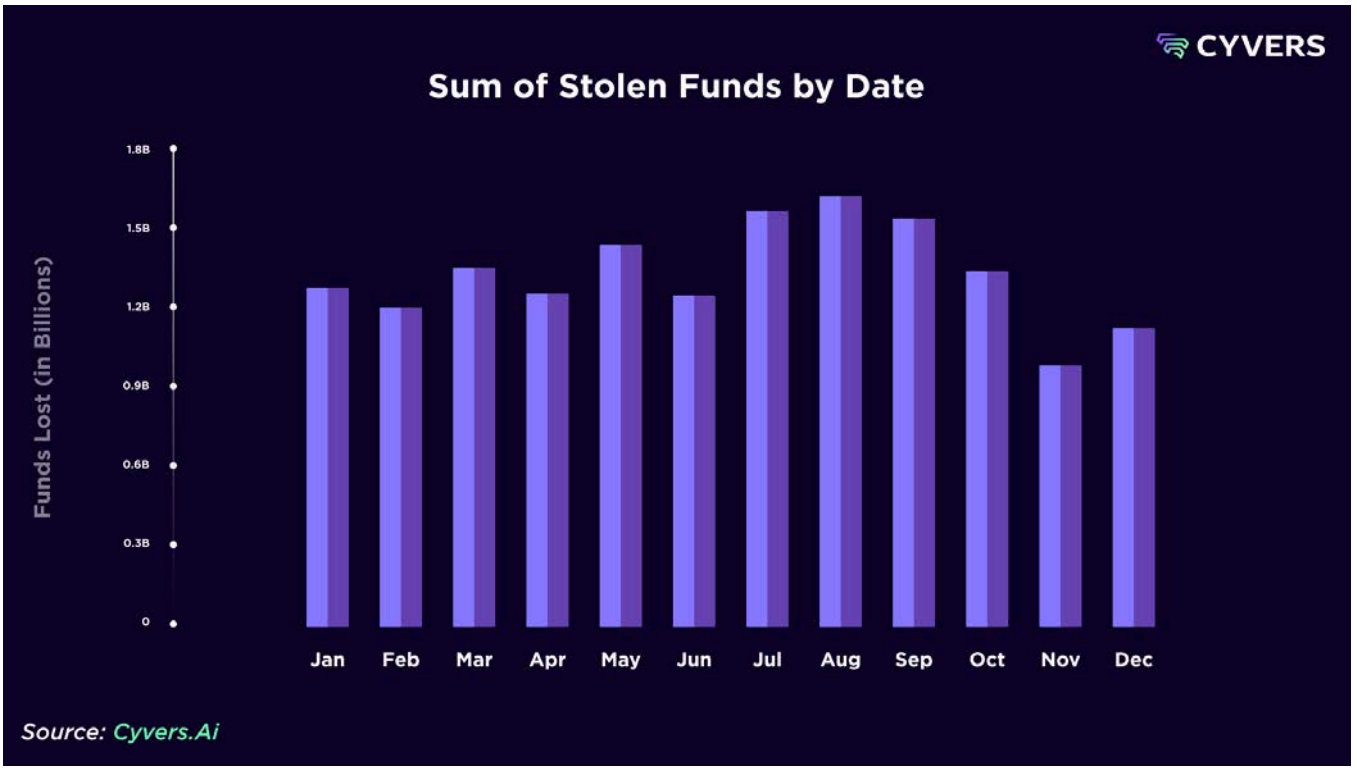
- **More than 19,000 active fraud networks**
- **More than 140 exchanges and trading venues affected worldwide**
- **Largest single fraud transaction: over 30.6 million dollars'** worth of ETH in a single transfer on August 7, 2025, on one of the world's largest centralized exchanges



These figures cover fraud broadly, both authorized and unauthorized, although social engineering based authorized fraud and pig butchering networks remain the most persistent and organized component of the problem.

Monthly distribution of stolen funds

Fraud losses in 2025 did not unfold evenly over the year. Stolen funds started at over $1.2 billion in January and eased slightly in February to a bit above $1.1 billion. From March to May, losses climbed again, holding in the $1.2 to $1.4 billion range and reaching a local high in May. After a modest pullback in June, the summer brought a new surge: July crossed about $1.5 billion, and August became the peak month at close to $1.6 billion in stolen funds. From there the curve flattened rather than collapsing, with September remaining near $1.5 billion, October slipping to around $1.4 billion, and November and December still recording roughly $1.0 to $1.2 billion each, well below the summer peak but clearly above the early year low.



Scale and Structure of Fraud Networks

The 2025 data confirms that crypto fraud is driven by professional, scalable operations, not isolated one-off scams. Over 18,800 active fraud networks reused infrastructure across hundreds of thousands of addresses and millions of transactions.

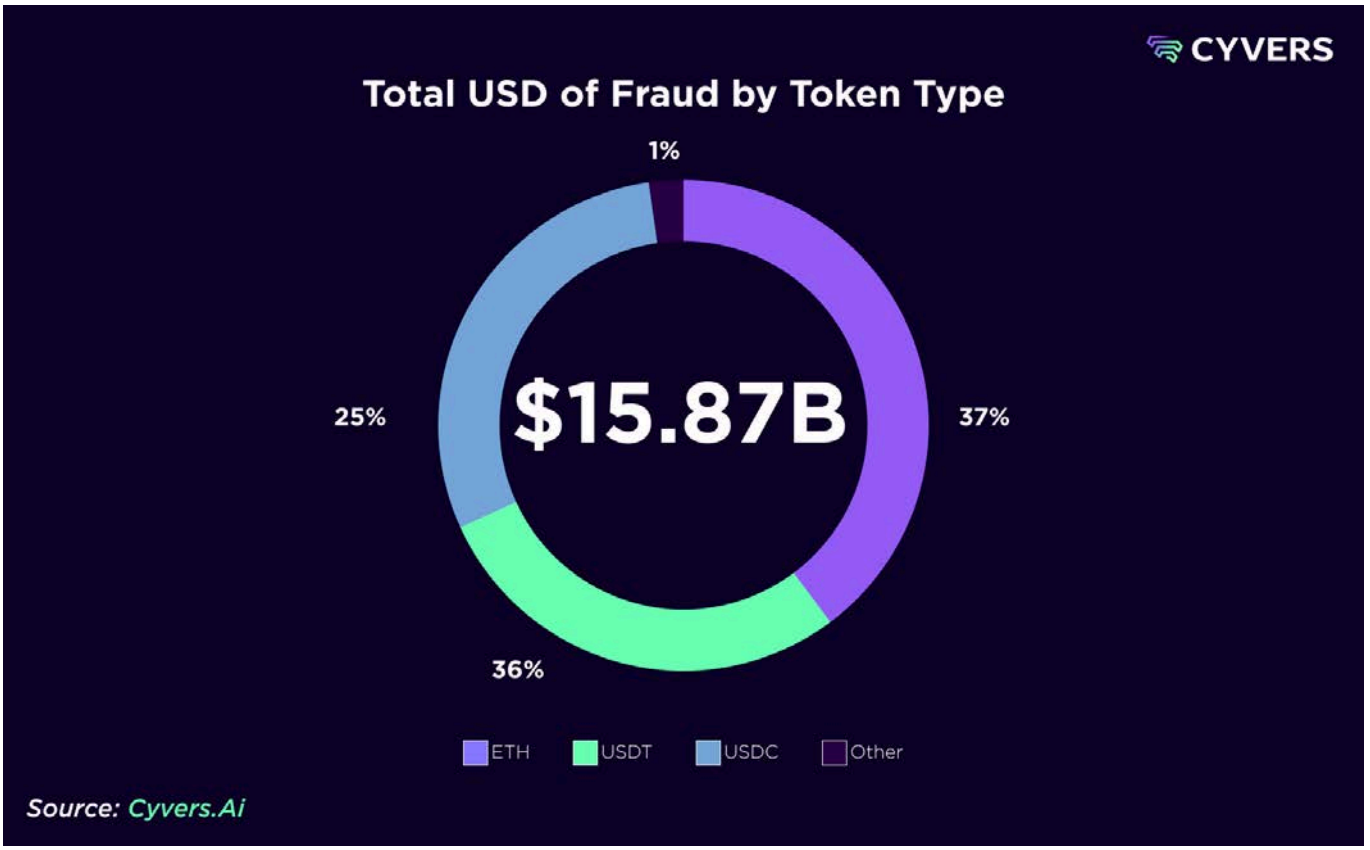
Typical patterns involve:

- Repeated use of clusters of addresses tied to the same scam operation.
- Cross platform movement that chains together multiple exchanges, PSPs, and off-ramps.
- Sophisticated social engineering that keeps victims engaged for weeks or months before the "cash out" moment.

Because the victim technically authorizes many of these transactions, traditional fraud controls that focus on compromised accounts are often blind to these flows. Real time behavioral analytics, graph analysis, and entity level risk scoring are required to catch these schemes before funds leave the platform.

Fraud by Asset Type

Fraudulent value in 2025 was highly concentrated in a small set of liquid, widely supported assets. Out of the more than $15 billion detected by Cyvers:

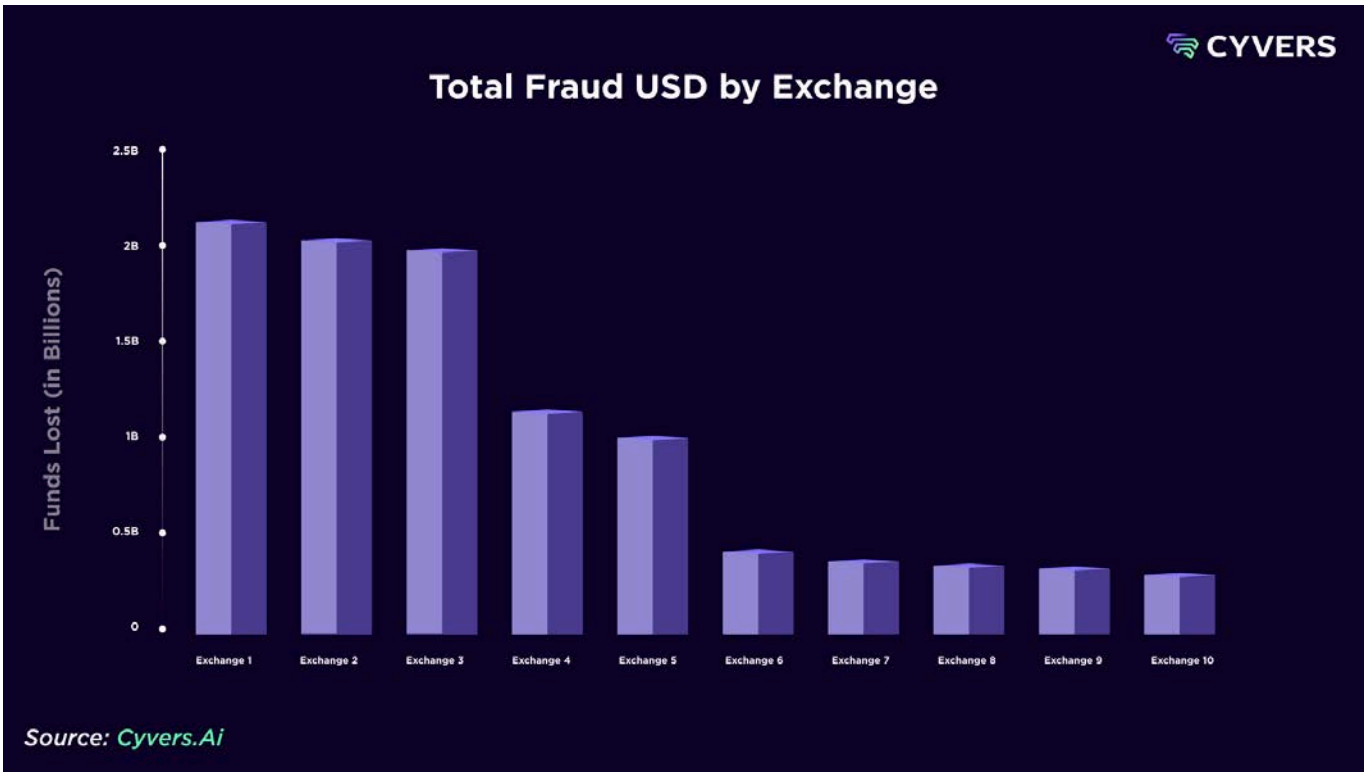


- **USDT** accounted for nearly 36% fraud-related bit more than one third of all fraud-related value.
- **ETH** represented over 37% billion, close to another third.
- **USDC** contributed over 25% billion, just under a third.
- **All other tokens combined** added around 1% billion, only a tiny fraction of the total.

Taken together, the two dominant dollar stablecoins carried well over two thirds of detected fraudulent value, while ETH added almost another third. The preference for these assets reflects their deep liquidity, tight integration with centralized and decentralized trading venues, and efficient fiat conversion. For fraud networks that need to move and launder large amounts of money quickly, they are the preferred rails.

Platform Exposure: Concentration of Risk

Fraud losses in 2025 were not evenly spread across the more than 140 exchanges and trading venues monitored by Cyvers. Instead, they were heavily concentrated in a relatively small group of systemically important platforms.



Key observations include:

- The single most exposed global exchange accounted for well over $2.3 billion of detected fraudulent flows, close to one fifth of the annual total.
- Three of the ten largest exchanges in the world together were responsible for almost half of all fraud volume routed through centralized platforms.
- Five of the top global exchanges, together with a major stablecoin issuer, accounted for more than 70% of all fraudulent value identified.

This concentration is partly a function of market share: fraudsters follow liquidity. However, it also reflects uneven maturity in fraud controls, analytics capabilities, and response processes across platforms. For the industry, it means that targeted improvements at a handful of large venues and one major issuer could significantly reduce overall losses.

What These Findings Mean for 2025 and Beyond

The 2025 figures confirm that crypto fraud has become an industrialized global enterprise that rivals traditional organized crime markets in size. Pig butchering remains the flagship model within authorized fraud, but it operates alongside a wide range of other schemes that all exploit the same core rails: liquid stablecoins, blue-chip assets, and large centralized exchanges.

For exchanges, wallets, PSPs, and financial institutions, the implications are clear:

- **Fraud is now a systemic risk**, not a marginal cost of doing business.
- **Authorized fraud must be treated as seriously as unauthorized fraud,** even when transactions are technically compliant and initiated by the user.
- **On-chain, real time detection and investigation capabilities are essential**, because off-chain reporting and user complaints cover only a small fraction of cases, and education alone cannot overcome deeply manipulative social engineering.

Platforms that integrate driven fraud analytics into their transaction flows can move from reactive case handling to preemptive prevention: stopping suspicious transfers before they settle, identifying exposure to fraud networks as they evolve, and reducing their share of the more than $15 billion fraud problem that defined crypto in 2025.

CYVERS

Regulation and Standardization Developments

Regulation and Standardization Developments

Global

International Regulatory Convergence

- **Key Developments**

  Policymakers are aligning crypto rules.Most major economies are building comprehensive frameworks for crypto and stablecoins. Global bodies, G20, FSB, IMF, IOSCO, BIS, are coordinating guidance. About 99 jurisdictions are implementing the FATF Travel Rule by 2025. 2025 marks a shift toward more consistent global oversight. International forums have made it a priority to address cross border risks with a coordinated and comprehensive approach. This push for convergence is evident in the widespread adoption of standards.

- **Implications**

  Convergence reduces regulatory arbitrage, supports uniform AML, KYC, licensing, and stablecoin reserves, and enables license recognition and cross border supervision. Greater certainty lets firms innovate with confidence. Investors and consumers benefit from clearer protections no matter where a crypto service is based. As countries synchronize their policies, the crypto industry gains greater legal certainty and can innovate with more confidence about what is allowed.

- **Why It Matters**

  Borderless assets need coordinated rules to protect consumers, markets, and stability. Consistent standards, including for stablecoins, signal a maturing sector and can build public trust. A globally coordinated regime means that major markets agree on baseline rules for consumer protection, market integrity, and financial stability. Convergence also signals the maturing of the crypto sector, it is being integrated into the traditional financial regulatory architecture rather than operating on the fringes.

- **Challenges and Criticisms**

  Implementation differs by country, creating gaps. One size may stifle innovation in developing markets. Some resist ceding sovereignty. Enforcement remains uneven, so effective, shared supervision is essential. The FSB warns that inconsistent implementation of its crypto framework may undermine its effectiveness and lead to regulatory arbitrage if some jurisdictions lag or enforce rules weakly. Developing countries often lack the resources for robust oversight, creating potential havens for unregulated activity.

FATF Travel Rule

- **Key Developments**

  By 2025, 99 jurisdictions have adopted or are adopting the Travel Rule for crypto. The EU applies it via the Transfer of Funds Regulation, the U.S. via FinCEN expectations, and guidance tightens definitions. The Industry has built secure data sharing solutions and best practices. This marks a dramatic increase in adoption since the rule was first recommended for crypto in 2019. By 2025, the Travel Rule has gone from theory to practice in a majority of key jurisdictions.

- **Implications**

VASPs need bank like compliance, KYC, and data exchange, increasing transparency and aiding investigations. Standards and interoperability are advancing, pushing hesitant jurisdictions to align. The overall effect is a more transparent ecosystem among regulated entities, which should make it harder for criminals to hop between exchanges without leaving a trail. International cooperation and common data formats are needed for effective exchange of information.

- **Why It Matters**

  The Travel Rule brings crypto toward AML parity with traditional finance, deters illicit finance, reduces arbitrage, and supports integration with regulated systems. It addresses the criticism that crypto is a haven for criminals by making movements more traceable. It sets the stage for more integrated financial systems where risk is assessed across both fiat and crypto transfers.

- **Challenges and Criticisms**

  Interoperability, thresholds, and unhosted wallets create gaps. Privacy and data security concerns persist. Enforcement is uneven, costs are high, and criminals adapt with mixers, bridges, and DeFi. Technical compatibility across hundreds of providers is complex, and thresholds vary by jurisdiction. Sophisticated actors already use techniques like cross chain bridges and privacy coins to evade detection.

United States

Digital Asset Market Clarity Act of 2025 (CLARITY Act)

- **Key Developments:**

  The Digital Asset Market Clarity Act of 2025 (H.R. 3633) advanced in the House during July 2025, moving through the Rules Committee, with text published on Congress.gov; the bill seeks to delineate when digital assets are securities vs. commodities and set a pathway for compliant token distribution and trading. Media coverage also notes separate House passage alongside stablecoin legislation, sending the market-structure debate to the Senate.

- **Implications**:

  If enacted, clearer jurisdictional lines between the SEC and CFTC could reduce enforcement uncertainty, enable exchanges and issuers to structure listings and disclosures with defined regimes, and support secondary-market liquidity for compliant tokens. Firms would still need robust AML, surveillance, and custody programs aligned to their asset's classification.

- **Why It Matters:**

  A federal market-structure framework is a prerequisite for institutional participation at scale; statutory clarity can unlock product development and risk management akin to other asset classes, while preserving investor protections. It also positions the U.S. to influence global norms on token classification.

- **Challenges and Criticisms:**

  Policy groups and security experts warn of AML and national-security gaps if the bill leaves DeFi or mixers under-addressed, urging stronger Treasury authorities and consistent controls across issuers. The bill's Senate path, potential amendments, and inter-agency coordination remain uncertainties.

NYDFS Blockchain Analytics Guidance for Banks (New York)

- **Key Developments:**

  On September 17, 2025, the New York Department of Financial Services issued an Industry Letter extending its 2022 blockchain analytics expectations (previously for virtual currency entities) to all NYDFS-regulated banking organizations and NYDFS-licensed foreign bank branches, requiring risk-based use of blockchain analytics tools where crypto exposures exist. Law-firm and press analyses highlight the expansion to mainstream banks and integration with third-party and cybersecurity risk management.

- **Implications:**

  Covered institutions must assess use-cases (e.g., payments, custody, counterparties), implement appropriate analytics tooling, integrate results into AML monitoring and sanctions screening, and update policies, vendor due-diligence, and governance, bringing bank-grade controls to crypto-adjacent activities. Expect examiner focus on model risk, data quality, and escalation procedures.

- **Why It Matters:**

  NYDFS is setting a high-water mark by normalizing blockchain analytics in traditional banking supervision, shrinking blind spots between fiat and crypto flows and improving interdiction of illicit finance. This move pressures national and other state regulators, and banks outside New York, to meet similar expectations.

- **Challenges and Criticisms:**

  Implementing analytics across legacy systems raises cost, data-integration, and false-positive challenges, especially for smaller institutions; banks must also manage privacy, vendor risk, and examiner scrutiny of methodologies. Scope boundaries (when activity is sufficiently “crypto-exposed”) will require careful interpretation.

The Strategic Bitcoin Reserve and the GENIUS Act

- **Key Developments**

  An Executive Order in March 2025 created a Strategic Bitcoin Reserve and a Digital Asset Stockpile, consolidating seized BTC for long term holding, not for sale, with budget neutral acquisition strategies and a feasibility study. The GENIUS Act, July 18, 2025, set a federal framework for payment stablecoins. Bank regulators oversee issuers, non banks can obtain an OCC license, and compliant stablecoins are not securities or commodities. The order also creates a stockpile for other seized digital assets and calls for strategies to possibly acquire more BTC in budget neutral ways. In short, the U.S. is both treating Bitcoin as a strategic reserve asset and creating guardrails for dollar pegged stablecoins as of 2025.

- **Implications**

  The Reserve legitimizes BTC as a strategic asset and raises custody standards. The GENIUS Act enables regulated USD stablecoins, supports payments integration, and may strengthen the dollar’s digital role. We may see an uptick in USD backed stablecoin offerings from banks or licensed entities, integration of stablecoins into payment systems, and possibly greater use of the dollar via digital tokens globally. It also raises the bar for crypto custody and security standards, as managing a sovereign BTC reserve requires robust infrastructure.

- **Why It Matters**

  The U.S. moves from reactive to strategic. The Reserve hedges against others' accumulation. The GENIUS Act, the first federal crypto law, clarifies oversight, enabling innovation with

protection. It provides the regulatory clarity that businesses and investors have long sought, delineating what is allowed and which agencies oversee which activities. It reflects a hedge, if Bitcoin truly is digital gold, the U.S. wants a stake in it.

- **Challenges and Criticisms**

  BTC volatility, custody risk persist, and budget-neutral growth may be limited. Critics fear manipulation or conflict with decentralization. The Act restricts issuance to permitted entities, possibly concentrating the market and chilling innovation. Global and domestic oversight coordination will be complex. Consumers might enjoy better protection, but crypto purists worry about heavy oversight and the exclusion of non bank innovators. Enforcement of the new law will also be a challenge, regulators will need to ramp up supervision for a new class of stablecoin issuers, and coordinating oversight will test the regulatory architecture.

European Union

MiCA and DORA in Action

- **Key Developments**

  MiCA, phased in during 2024 and 2025, and DORA, effective January 2025, form the EU's twin pillars. MiCA sets licensing, consumer protection, and market abuse rules. DORA mandates cybersecurity, incident reporting, and resilience. AML rules, including the Travel Rule, run in parallel. MiCA establishes uniform rules across all 27 EU member states for issuers and service providers. By mid 2025, member countries began issuing MiCA licenses that grant firms passported access EU wide.

- **Implications**

  Passporting unifies the market and attracts global firms. DORA raises reliability to bank-like standards. Arbitrage narrows, and EU practices may shape global norms. Companies now have clarity on requirements, they must implement consumer protection, prudential safeguards, and disclosures. European regulators are coordinating oversight to ensure consistency.

- **Why It Matters**

  The EU shows that comprehensive regulation is feasible, restoring trust after market failures and encouraging responsible innovation across the single market. By aiming to bring crypto under the same regulatory umbrella as traditional finance, the EU asserts that investor protection and market integrity should be no less in crypto. If successful, the EU's comprehensive regime could bolster legitimacy and open the door for new, compliant offerings.

- **Challenges and Criticisms**

  Enforcement varies across members, raising race to the bottom. DeFi and many NFTs sit outside the scope. Compliance costs and privacy concerns persist, and agility is needed to keep pace. The challenge is ensuring uniform enforcement across member states. There is a risk of regulatory rigidity, technology evolves quickly and laws can become outdated.

United Kingdom

Draft Financial Services and Markets Act (Cryptoassets) Regulations 2025

- **Key Developments:**

  On April 29, 2025, HM Treasury published a near-final draft statutory instrument, Financial Services and Markets Act 2000 (Regulated Activities and Miscellaneous Provisions) (Cryptoassets) Order 2025 plus a policy note, to bring specified cryptoasset activities into the UK regulatory perimeter, with industry feedback requested by May 23, 2025. The draft sets out new regulated activities and updates the RAO framework to capture cryptoasset intermediation under FCA oversight.

- **Implications:**

  UK-facing crypto businesses will need authorisation (or vary permissions), implement FCA standards for conduct, disclosures, and prudential/operational resilience, and align compliance with other UK regimes (e.g., financial promotions, AML). Non-UK firms targeting UK users must assess territorial scope and whether activities are "carried on in the UK," tightening cross-border access.

- **Why It Matters:**

  The draft order provides long-sought clarity on the UK's "activities-based" approach, reducing uncertainty after years of piecemeal measures and moving closer to EU-style comprehensive oversight. This enables boards and product teams to plan licensing, risk, and go-to-market strategies with greater predictability.

- **Challenges and Criticisms:**

  Timing and final scope remain open pending consultation and parliamentary process; firms face cost and complexity to map activities and upgrade systems. Divergences from EU MiCA or other hubs could add fragmentation risks for global platforms serving multiple regions.

United Arab Emirates (Dubai)

VARA Virtual Asset Rulebook Updates 2025

- **Key Developments:**

  In May–September 2025, Dubai's Virtual Assets Regulatory Authority (VARA) issued rulebook revisions tightening AML/CFT expectations, codifying FATF Travel Rule obligations, and sharpening compliance and risk-management controls across VASPs; the public "View Revision Updates" log highlights new and amended provisions (e.g., Compliance Management and AML/CFT sections) dated 19 May 2025. These updates reinforce customer due diligence, data sharing for transfers, and operational risk controls that align with international standards.

- **Implications:**

  Exchanges, custodians, and issuers operating in Dubai must evidence continuous monitoring and Travel Rule compliance, enhance internal controls, and document governance and testing raising the minimum operational baseline and narrowing gaps with leading global regimes. The clearer, updated rulebooks also facilitate consistency for firms seeking multi-jurisdiction compliance programs anchored in FATF norms.

- **Why It Matters:**

  As one of the most active regional hubs, Dubai's more prescriptive rulebooks signal that market access comes with bank-grade surveillance, custody discipline, and cross-border data obligations, improving investor protection and supervisory confidence. The changes also support the UAE's broader push to align with international AML standards and strengthen its reputation with global partners.

- **Challenges and Criticisms:**

  Implementing real-time monitoring and Travel Rule data exchange can be costly for smaller VASPs, and harmonizing controls across complex group structures adds operational friction. Consistent enforcement and technical interoperability with counterparties abroad remain practical pressure points.

APAC

Regulatory Implementation and Consolidation

- **Key Developments**

  Hong Kong passed a landmark stablecoin bill on May 21, 2025, with the regime taking effect on August 1, 2025, and the HKMA signaling that the first licenses are likely in early 2026. Indonesia shifted crypto oversight from Bappebti to the Financial Services Authority, OJK, effective January 10, 2025, formalizing a new licensing and supervisory perimeter. South Korea's FSC issued lending guidelines on September 5, 2025, capping crypto lending interest at 20 percent and banning leveraged loans, while preparing the second phase of a broader virtual asset law for the National Assembly session. Australia published a March 2025 policy statement outlining draft legislation in 2025 for digital-asset platform licensing and a payment stablecoin framework, and Singapore's earlier stablecoin rules continued to serve as a regional reference point.

- **Implications**

  The region is converging on clearer licensing and prudential requirements, from fiat-referenced stablecoin regimes in Hong Kong to lending risk controls in South Korea, which raises compliance baselines for exchanges, custodians, and issuers. Indonesia's centralization of supervision under OJK and Australia's move toward platform and stablecoin rules point to tighter governance, more predictable market access, and stronger consumer protection, while Singapore's mature framework anchors regional expectations.

- **Why It Matters**

  APAC hosts several of the world's most active crypto markets, so formalized stablecoin, lending, and platform regimes in Hong Kong, Korea, Indonesia, Australia, and Singapore will shape global norms on reserves, disclosures, and operational resilience. These steps aim to reduce market abuse and illicit finance risk, increase investor confidence, and create passportable or at least interoperable pathways for institutional participation across major Asian hubs.

- **Challenges and Criticisms**

  Timelines and scope remain uneven, for example Australia has outlined its approach, but as of late summer 2025, exposure drafts had not yet been released, and South Korea still needs to pass phase-two legislation. Implementation costs may burden smaller firms, while restrictive lending caps and tightly controlled stablecoin regimes could curb product innovation or push activity to less regulated venues until rules are fully harmonized.

Standardization

Real-Time Monitoring Becomes the Norm

- Key Developments

  In 2025, real-time monitoring is expected. MiCA requires continuous market abuse detection. AML regimes push ongoing monitoring and perpetual KYC. Exchanges deploy KYT tools, regulators use analytics, and DeFi monitoring and data standards evolve. Continuous surveillance of blockchain activity is being mandated in many regimes. Keeping a live eye on transactions and reacting promptly is the norm, not the exception.

- Implications

  Faster detection improves risk mitigation and fund freezes, but generates heavy alert volumes and staffing needs. Strong programs build trust, raise the baseline, and protect investors. Real-time systems generate a lot of alerts and data, requiring robust internal processes and skilled analysts. Proactive monitoring can stop fraudulent transactions in their tracks.

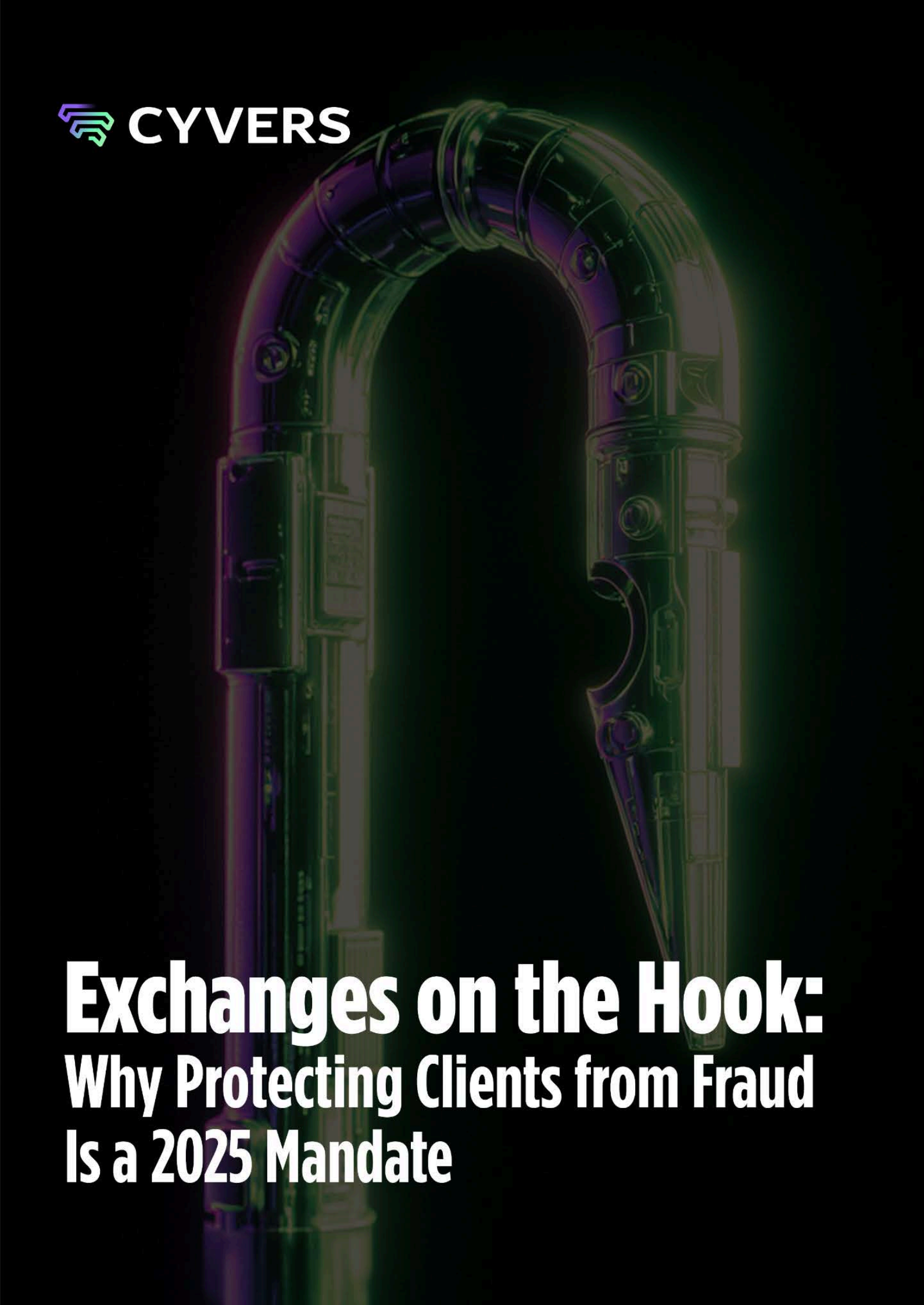
- Why It Matters

  Real-time oversight matches crypto's speed, moves compliance from reactive to preventive, leverages AI and RegTech, and supports public confidence and integration with traditional finance. Regulators are no longer content with after-the-fact reporting, they want preventive or immediate measures. This signals that crypto is converging with the expectations of global financial markets.

- Challenges and Criticisms

  Costs, privacy, DeFi coverage, adversary adaptation, vendor concentration, and potential market impact require careful calibration and collaboration. Smaller companies might struggle with the cost and expertise needed to implement and maintain sophisticated systems. It is a constant arms race as criminals pivot to obfuscation techniques.

CYVERS



Exchanges on the Hook:
Why Protecting Clients from Fraud Is a 2025 Mandate

Exchanges on the Hook: Why Protecting Clients from Fraud Is a 2025 Mandate

Fraud Surges to Record Highs in 2025

Cryptocurrency fraud escalated dramatically, making 2025 one of the worst years on record for fraud losses. In the United States alone, the FBI reported that victims lost $9.3 billion to crypto-related fraud in 2024, a 66% increase from the prior year. Seniors were especially hard-hit, with Americans over 60 accounting for $2.8 billion of those losses. This trend has only accelerated in 2025. According to Cyvers data, over $15 billion were stolen globally in more than 750,000 incidents.

Much of this spike is due to the emergence of well-funded fraud networks, working primarily in South-East Asia. They leverage novel fraud tactics, prompted by emerging artificial intelligence technology - allowing perpetrators to present themselves as legitimate people of all nationalities and languages.

Sophisticated fraud operations like “pig butchering” - long-con investment scams where criminals groom victims before stealing their funds - are scaling rapidly in 2025, contributing to a broader explosion of crypto fraud. Compliance firm reports warn that ***scams have become one of the most lucrative forms of illicit crypto activity***, continually growing in scope and sophistication. In short, clients are facing greater risks than ever of being defrauded, and exchanges can no longer view these losses as merely the customer’s problem.

Regulators Shift Liability onto Exchanges

Financial authorities in major jurisdictions have taken note of this fraud epidemic – and are responding by shifting more responsibility and liability onto exchanges and payment providers. In the UK, ***authorized push payment*** (APP) ***fraud*** (where victims are tricked into sending money to scammers) has become the country’s largest category of payment fraud by number and value. To combat this, regulators enacted new rules effective October 2024 that mandate reimbursement to victims. Under the Payment Systems Regulator’s directive, virtually all payment service providers (banks and fintechs using the Faster Payments network) must fully refund consumers defrauded by APP scams, up to £85,000, within just days of the fraud report. This aggressive policy effectively puts the onus on financial institutions to absorb fraud losses and ***incentivizes them to prevent scams in the first place.***

In the United States, regulators and courts are likewise pushing crypto platforms to take accountability. The U.S. Treasury’s Financial Crimes Enforcement Network (FinCEN) has explicitly warned crypto exchanges that they must detect and prevent emergent threats like pig butchering and elderly financial exploitation. Exchanges are considered money service businesses under the Bank Secrecy Act (BSA) and are legally required to implement effective anti-money laundering programs – including ***actively monitoring transactions for suspicious activity and taking action to prevent fraud and abuse.*** In a groundbreaking recent case, a U.S. federal court signaled it is prepared to hold exchanges liable if they fail in this duty.

In September 2025, the District Court for the Northern District of California ruled that victims of a “pig butchering” crypto scam could pursue claims against the exchange that the fraudsters used. The court found that by allegedly “failing to police [its] platform for money laundering and financial crime,” the exchange could have violated the BSA and consumer protection laws. This decision is a legal game-changer – it ***opens the door for defrauded consumers to sue exchanges*** for restitution if criminals used those exchanges to facilitate fraud. In short, U.S. courts are making it clear that the “hear no evil” approach will no longer shield crypto companies from liability when users are scammed.

Moreover, the US Consumer Financial Protection Bureau (CFPB) is considering new regulations aimed at imposing reimbursement for financial services companies failing to prevent hacks, scams and fraud on their platforms.

Meanwhile, the European Union's new Markets in Crypto-Assets (MiCA) regulation is raising the bar for consumer protection across EU exchanges. MiCA imposes strict obligations on crypto-asset service providers to safeguard users' funds and prevent fraud. For example, exchanges and custodians must segregate client assets, maintain robust cybersecurity controls, and monitor suspicious transactions and market abuse. The regulation explicitly targets deceptive practices – requiring transparent disclosures and banning misleading promotions – to protect investors from scams. Transparency, accountability, and proactive fraud detection are now legal requirements in the EU's crypto market oversight. Exchanges that fall short risk hefty penalties or loss of their license under MiCA's enforcement regime.

Asian jurisdictions, including Singapores' MAS, Hong Kong's HKMA and SFC and United Arab Emirates' VARA have issued similar consumer protection rules.

The common thread in these developments across the mentioned jurisdictions is a clear message: exchanges and financial platforms will be held accountable for customer fraud losses. Governments are effectively saying ***"if you don't protect your users from scams, we will make you pay".*** Whether via mandated reimbursements, lawsuits citing compliance failures, or stringent regulations, the liability for client fraud is shifting from the individual victims to the institutions facilitating the transactions. This is a paradigm shift – one that directly affects exchanges' bottom lines and legal exposure.

Business and Reputational Imperatives

Beyond regulatory obligations, there is a strong business case for exchanges to care deeply about clients being defrauded. At the most basic level, customer trust is the foundation of an exchange's success – and nothing erodes trust faster than users losing their life savings to scams or hacks on an exchange's watch. Executives should recognize that ***fraud losses harm both the customer and the platform.*** A defrauded client may never return to trading (or may withdraw remaining assets out of fear), translating to lost revenue for the exchange. Worse, if an exchange develops a reputation as a haven for scammers or as an unsafe place for retail users, it can trigger an exodus of clients and deter new sign-ups. In contrast, taking a proactive stance on user protection can become a competitive advantage. In an industry plagued by security incidents, an exchange that actively safeguards its customers and swiftly addresses fraud can attract more business from security-conscious traders and institutional partners.

There are also significant financial risks to the exchange itself when clients are defrauded. The ***legal*** costs can mount quickly: defending class-action lawsuits or regulatory enforcement actions related to fraud can cost millions in litigation and remediation. Even if an exchange user agreement disclaims liability for scams, that won't necessarily stop determined plaintiffs or regulators from pursuing claims. Preventing fraud is simply far more cost-effective than reacting to it after the fact. Every scam thwarted or hack averted saves the exchange potentially huge payouts, legal fees, and emergency incident response expenses.

Reputation management is another factor. High-profile fraud incidents draw negative press and scrutiny from authorities. Exchanges that appear negligent or indifferent to customer losses will endure reputational damage that can be hard to repair. On the flip side, exchanges that collaborate with law enforcement to crack down on fraud and that assist users who have been victimized demonstrate corporate responsibility. This fosters goodwill and loyalty among customers, regulators, and the broader community. In an era where brand trust equals market share in financial services, investing in fraud prevention is as much an operational necessity as it is an ethical one.

Proactive Strategies to Protect Users (and the Exchange)

Given the clear regulatory and commercial incentives, ***what concrete steps can exchanges take*** to shield their clients from fraud? The emerging best practices involve a mix of advanced technology, AI-powered real-time risk assessment, and coordinated response – a multilayered defense akin to what banks use but tailored to crypto's unique risks.

Cyvers detects and disrupts on-chain fraudulent activity by combining **topological AI, geometric anomaly detection**, and **real-time blockchain analytics**. It delivers:

1. **Real-Time Fraud Monitoring**
    - Detects interaction with wallets affiliated with fraud networks
    - Monitors hot wallets and on-chain activity in real time

2. **Pre-Transaction Screening (Address Screening API)**
    - Screens destination addresses **before** funds leave the platform
    - Prevents users from transferring funds to scam addresses

3. **Fraud Investigation & Reporting Tools**
    - Provides full backtracking of funds and wallet interaction history
    - Maps fraud networks and laundering paths to support compliance and recovery

Conclusion: Protecting Clients Is Protecting Your Business

In light of the 2025 landscape, it has never been clearer that exchanges must care about their clients being defrauded – because the consequences now land at the exchange's doorstep. The days of crypto platforms taking a hands-off approach to user fraud are over. Regulators across Western markets are actively enforcing a "duty of care" that requires exchanges to detect and prevent scams, under threat of legal liability and hefty costs. Customers, for their part, are gravitating toward platforms that make them feel safe and protected.

Exchanges that rise to the occasion by prioritizing fraud prevention will not only avoid fines and lawsuits but also reap tangible benefits: fewer incidents and emergency "fire drills," stronger user loyalty, and smoother compliance audits. The investments in real-time monitoring, smarter risk controls, and rapid response mechanisms pay for themselves by dramatically reducing loss events – which in turn lowers operational stress and safeguards revenue. In cryptocurrency's trust-driven industry, an exchange's reputation can be its most valuable asset.

By championing client protection and staying one step ahead of fraudsters, exchange executives and their fraud/security teams can uphold that reputation while meeting their regulatory obligations. The bottom line is simple: protecting your users from fraud is no longer just good PR or "the right thing to do" – in 2025, it's a core mandate for staying in business. An exchange that protects its customers is ultimately protecting itself.

CYVERS

Multisig Is Not a Panacea:

Why simple co-signers are not enough to prevent hacks?

Multisig Is Not a Panacea: why simple co-signers are not enough to prevent hacks

Executive brief

2025 proved that multisig by itself does not stop catastrophic loss. The largest exploit in crypto history, the Bybit exploit, was executed by tricking multiple operators into approving a malicious Safe wallet upgrade, then draining about 1.5 billion dollars from an exchange treasury. The first half of 2025 became one of the worst periods on record for hacks at 1.9 billion dollars lost, and mid-year reporting highlighted a wave of failures and misconfigurations around multisig operations. The pattern is clear: static rules and "second signature" checks are too easy to bypass when attackers control context. Smart, secure co-signers that simulate, score, and enforce policy at runtime are now table stakes.

Why simple co-signers and vanilla multisig failed in 2025

1) Signers lacked context at approval time: In the Bybit incident, operators approved what looked like a routine action, yet it was a malicious multisig upgrade that handed control to the attacker. The issue was not only the cryptography, it was the absence of runtime validation of the transaction's true effects.

2) UI deception and blind signing: Postmortems describe interface level tricks that made destinations and intents look benign. When humans cannot see balance deltas and state diffs before signing, a second signature only doubles the chance of approving the same trap.

3) Admin sprawl and role abuse: Several 2025 exploits involved elevated privileges or misconfigured signer roles that enabled minting or upgrades. Multisig can concentrate power if roles and policies are not continuously verified at the moment of action.

4) Scale and velocity outpaced manual checks: Exchanges faced rapid, cross-chain cash-outs. January and February alone drove a record quarter, which shows that human review windows cannot keep up without automated, inline controls.

What is a smart, secure co-signer

Cyvers rolled out its secure co-signer in mid-2025. This is not a rubber stamp; it is an active control layer that understands what a transaction will do, who it touches, and whether it violates policy.

- **Pre-execution simulation:** Intercept every payload, simulate the transaction, compute balance changes and contract state diffs, and compare the expected outcome with what will actually settle. Approve only if the simulation and intent match.
- **Risk scoring with real-time intelligence:** Enrich approvals with multi-hop counterparty and contract risk, including links to known exploit infrastructure, sanctioned clusters, and scam rings. Block or step up when risk exceeds thresholds.
- **Policy-aware signing:** Enforce custom rules at runtime, for example size limits by asset and chain, destination allowlists, upgrade and module-install restrictions, treasury timelocks, and business hour constraints.
- **Human-readable diffs for operators:** Render clear, signer friendly summaries that eliminate blind signing, then co-sign clean transactions in milliseconds to preserve operational speed.
- **Compatibility with existing custody:** Drop in alongside MPC and multisig stacks, including common enterprise wallet platforms and hardware devices, so teams gain prevention without rebuilding custody.

- **Audit trail and fail-secure defaults:** Log every simulation, decision, and policy evaluation, and fail secure if the co-signer cannot validate state, so attackers cannot exploit outages.

Implementation blueprint, tailored for 2026 realities

CeFi treasuries: Route every treasury movement and every module or upgrade action through the co-signer, require two independent channels for high risk approvals, and enable just-in-time privileges with time-bounded scopes.

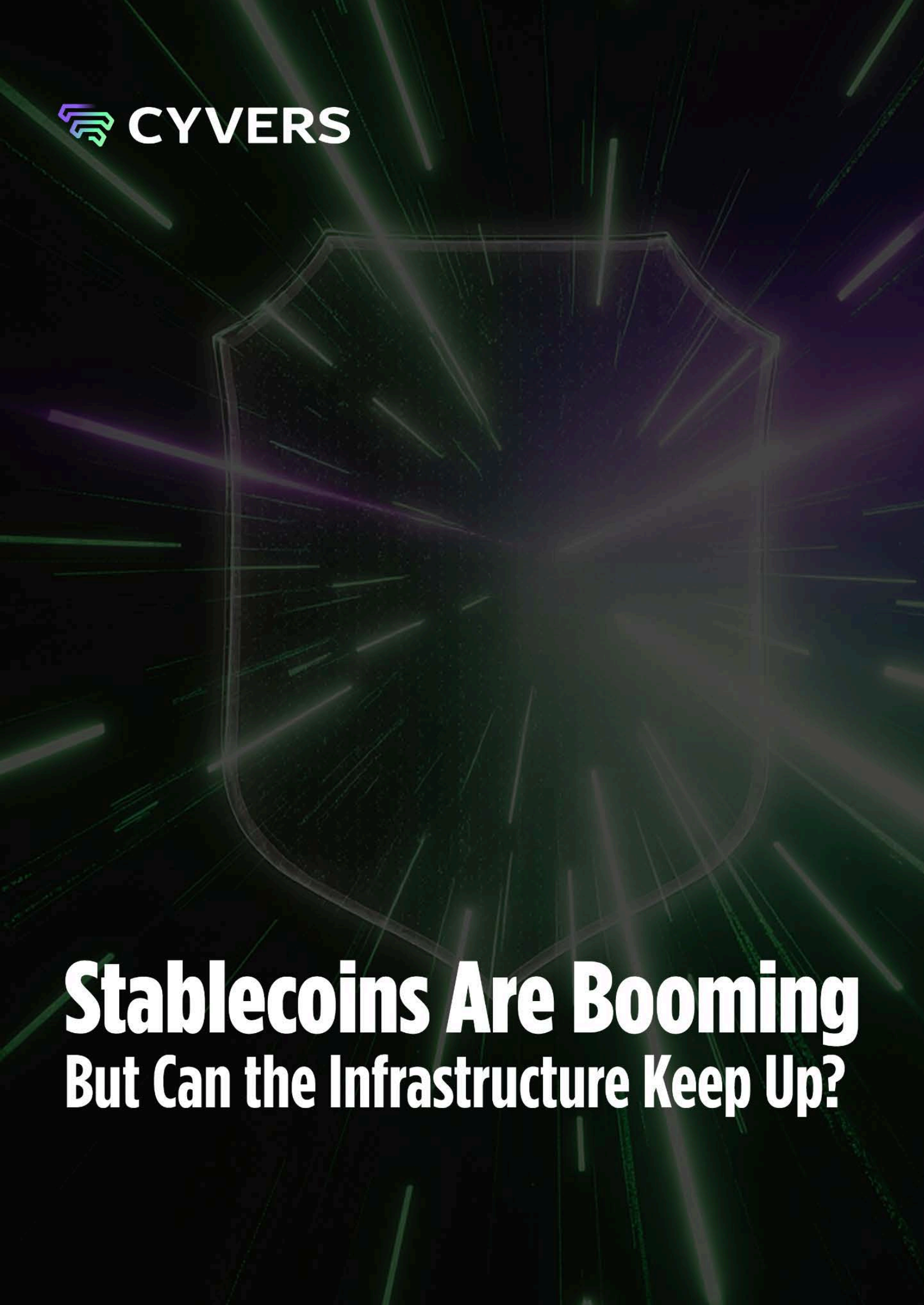
Protocols and foundations: Treat governance and operations transactions like cash movements, simulate and gate role changes, oracle or bridge permissions, and emergency functions, then publish signed audit artifacts for community trust.

Hardware wallet workflows: Pair clear signing with transaction checks that display human readable consequences, then require the co-signer's verdict before finalizing the signature.

Bottom line

Multisig and basic co-signing increase friction for attackers, but they do not validate intent, identify sophisticated social engineering attacks or enforce complex policy. 2025's largest breaches were approvals problems, not key problems. The way forward is a smart, secure co-signer that simulates, scores, and decides in line with business and compliance rules, at the exact moment value moves.

CYVERS



Stablecoins Are Booming

But Can the Infrastructure Keep Up?

Stablecoins Are Booming- But Can the Infrastructure Keep Up?

2025 proved that multisig by itself does not stop catastrophic loss. The largest exploit in crypto history, the Bybit exploit, was executed by tricking multiple operators into approving a malicious Safe wallet upgrade, then draining about 1.5 billion dollars from an exchange treasury. The first half of 2025 became one of the worst periods on record for hacks at 1.9 billion dollars lost, and mid-year reporting highlighted a wave of failures and misconfigurations around multisig operations. The pattern is clear: static rules and “second signature” checks are too easy to bypass when attackers control context. Smart, secure co-signers that simulate, score, and enforce policy at Stablecoins are no longer experimental. In 2025, they’ve become foundational to the digital asset economy, facilitating over $50 trillion in on-chain volume in 2025. With regulatory frameworks like the U.S. GENIUS Act and Europe’s MiCA unlocking institutional entry, the ecosystem is rapidly professionalizing.

Western Union, for example, is launching a USD-pegged stablecoin designed for cross-border payments, while financial institutions across Latin America and Asia are integrating stablecoins into remittance corridors, B2B payments, and treasury operations.

But the velocity of adoption has come with mounting exposure. In H1 2025 alone, the Web3 ecosystem saw $2.47 billion in stolen crypto, driven by exploits that weaponized or abused stablecoins directly - whether via smart contract manipulation, scam payouts, or laundering pathways. The Bybit hack, a ~$1.5 billion theft attributed to North Korean actors, is the most visible example, but it’s part of a broader pattern: fraud, security gaps, and compliance failures are growing in frequency and scale.

Stablecoins enable efficiency, but they also introduce risk. Fraud networks now target stablecoin holders with social engineering, address poisoning, romance and investment scams, and other malicious activities.

Meanwhile, compliance teams are struggling to keep up with regulatory expectations for real-time AML, sanctions screening, and traceability.

The bottom line: the infrastructure powering stablecoins needs to evolve fast.

What the Ecosystem Needs Now: Real-Time, Unified Risk Management

To sustainably scale, the stablecoin ecosystem requires an integrated approach to:

Security

The speed of blockchain leaves no margin for manual intervention. Transactions must be simulated, assessed, and scored before execution to prevent the danger arising from blind-signing, as well as to stop exploits such as oracle manipulation, flash-loans, protocol hacks.

Fraud Prevention

The human layer is often the weakest. Attackers exploit social trust, user inattention, or wallet mechanics to trigger irreversible transfers. The ability to screen addresses, detect fraud topology, and intervene during withdrawal flows is now essential. Stablecoins are already the go-to tokens for fraudulent transactions. This trend is expected to grow with the surge of offered stablecoins.

AML & Compliance

Institutions are facing increasing pressure to meet Travel Rule standards, avoid processing illicit funds, and screen counterparties in real time. For stablecoin issuers and custodians, traceability and accountability are becoming compliance baselines.

Cyvers: Full-Spectrum Threat Prevention for Stablecoin Infrastructure

Cyvers has emerged as a purpose-built platform to meet this new standard. Its AI-powered, real-time engine monitors the full transaction lifecycle - from pre-transaction validation to post-incident investigation - and provides tailored tooling for every stakeholder in the stablecoin economy.

Here's how Cyvers maps to today's emerging challenges:

Ecosystem Role	Challenge	Cyvers Capability
Issuers	Treasury misuse, illicit mint flows	Live mint surveillance + AML-grade counterparty risk screening
Settlement Chains	Network-level exploit detection	Early-warning systems for malicious flow anomalies
Bridges	Cross-chain attack vectors	Cross-chain exploit defense and real-time tracing
Wallets & Custodians	APP fraud, key leakage, insider threats	Pre-chain firewall + hot wallet breach monitoring
Payments	Scam payout destinations	Destination address screening before approval
Exchanges	Fraudulent cash-outs, sanctions exposure	Hot wallet protection + address reputation scoring
DeFi / Liquidity	Flash-loan & oracle-based exploits	Smart contract simulation + threat detection for TVL protection
Tokenization / RWAs	Tainted asset flow, layering	Asset provenance and illicit-flow tracing
Insurance	Poor breach forensics, claim complexity	High-fidelity incident feed and root-cause analysis

Fraud Detection and AML Are Built In, Not Bolted On

Cyvers isn't just about stopping hackers - it's also designed to address the **systemic fraud risks** that stablecoins are increasingly exposed to:

- **Fraud Network Detection:** Using graph analysis and geometric AI, Cyvers flags clusters of scam activity in real time—detecting pig butchering, phishing, and social engineering campaigns before funds are lost.
- **Address Screening API:** Integrated into exchange and wallet flows, this API blocks interaction with known scam, mixer, or sanctioned addresses, preventing both user loss and platform liability.
- **Transaction Risk Scoring:** Every transaction and address is continuously scored based on behavioral patterns, sanction links, and counterparty risk, enabling automated escalation and review.
- **AML and Regulatory Reporting Tools:** Cyvers supports forensic tracing, KYC-AML integrations, and Travel Rule compliance by mapping transaction provenance across chains. In recent cases, Cyvers tooling has helped platforms freeze or recover illicit funds in collaboration with authorities.

A Trusted Layer for a Maturing Market

Cyvers has already secured over **$30 billion in assets** across the Web3 space, with more than **$600 million in client losses prevented** in 2025. The platform flags **1 million+ malicious addresses weekly**, supports incident response for Tier 1 institutions, and is deployed by custodians, exchanges, and DeFi protocols alike.

This isn't just about reducing financial risk; it's about enabling confidence. Stablecoins are at a turning point: poised to power on-chain FX, global payments, and tokenized finance. But without a foundation of real-time security, fraud detection, and compliance, that promise can't be fulfilled.

The future of stablecoins depends on trust and trust depends on infrastructure.

Cyvers is helping build it.


CYVERS
Leveraging AI Agent-Powered SOCs to Enhance Web3 Security in 2025

Leveraging AI Agent-Powered SOCs to Enhance Web3 Security in 2025

The year 2025 saw an unprecedented wave of crypto-related cyberattacks and scams that tested the limits of traditional security operations. From a record-shattering $1.5 billion exchange hack to sprawling “pig butchering” scam networks, threat actors outpaced conventional defenses. Security Operations Centers (SOCs) struggled to keep up amid alert overload and increasingly sophisticated attack techniques. In response, a new paradigm emerged: AI agent-powered SOCs. These autonomous digital analysts proved capable of detecting subtle anomalies, triaging floods of alerts, and orchestrating rapid incident response in ways human-only teams could not. This article examines how AI-driven SOC agents helped counter 2025’s top Web3 threats – and why they represent a pivotal upgrade over traditional SOC models.

2025’s Web3 Threat Landscape: Big Hacks and Bigger Scams

Exchange Heist – Bybit’s $1.5B Hack:

In February 2025, Dubai-based exchange Bybit suffered the largest cryptocurrency theft in history, with hackers siphoning approximately $1.46 billion in cryptoassets. Investigators linked the breach to North Korea’s Lazarus Group and discovered a multi-pronged attack chain. The adversaries combined social engineering and supply-chain tactics – tricking a software developer into running a malicious update – to infiltrate Bybit’s environment. Once inside, they stole cloud credentials, bypassed multi-factor authentication, and even planted a covert JavaScript snippet that diverted funds during a high-value transfer. Within hours of the heist, the perpetrators dispersed the loot across dozens of wallets and used decentralized exchanges and mixers to launder the assets. This rapid, complex attack overwhelmed traditional defenses, highlighting how quickly humans can be outmaneuvered.

Global Scam Networks – Pig-Butchering Schemes:

A less overt but equally damaging threat in 2025 was the surge of “pig butchering” crypto investment scams. These schemes, often run from scam compounds in Southeast Asia, dupe victims through long-term social engineering – cultivating trust via romance or mentorship before stealing their assets. Losses have been staggering: in 2024, U.S. victims reported over $5.8 billion lost to cryptocurrency investment fraud (largely pig butchering).

In 2025, law enforcement struck back. A U.S. Secret Service-led operation seized $225 million from pig-butchering rings – the largest crypto seizure in the agency’s history – signaling a new level of collaboration between authorities and industry. However, the scammers also upped their game. They leveraged generative AI to scale and personalize their cons, churning out convincing fake profiles and messages en masse. Blockchain analysts noted that the rise of pig butchering, abetted by AI-driven content, likely pushed crypto scam revenue to record highs in 2024. Put simply, criminals are weaponizing AI, forcing defenders to respond in kind.

Phishing and Social Engineering Windfalls:

Even individual investors proved lucrative targets. On August 19, 2025, a single Bitcoin holder lost 783 BTC – worth about $91 million – to a phishing scam. Posing as hardware wallet support staff, scammers convinced the victim to divulge their recovery seed, then immediately drained the wallets and laundered the funds through crypto mixers. This became one of the largest social-engineering heists on record and a cautionary tale that even well-resourced individuals remain vulnerable to human-targeted attacks.

Corporate victims were not spared either: in May, Coinbase disclosed that insiders at a support contractor were bribed by attackers, exposing user accounts and enabling an estimated $400 million

theft via unauthorized transfers. These incidents underscore that clever social engineering – whether by impersonating trusted support or exploiting insider access – can defeat the best technical controls if not caught in time.

DeFi Drainers – Smart Contract Exploits:

Decentralized finance platforms faced relentless assaults in 2025, often via vulnerabilities that traditional code audits missed. A prime example was the Cetus DEX hack on the Sui blockchain: attackers created fake token contracts to manipulate liquidity pools and drain about $220 million in assets.

By spoofing token metadata and tricking the protocol's smart contracts, they bypassed security checks and emptied funds in minutes. Earlier in the year, flash loan exploits and logic flaws hit other DeFi protocols – for instance, an Abracadabra Money breach in March allowed $13 million to be stolen by exploiting a complex sequence of contract calls. These on-chain attacks moved at machine speed, leaving defenders little time to react. They also revealed gaps in conventional defenses: static audits and rule-based monitors often failed to detect novel attack patterns or private key compromises in real time.

Why Traditional SOCs Fell Behind

The onslaught of 2025 exposed how conventional SOCs – reliant on human analysts and predefined rules - struggle against fast, sophisticated threats. Key limitations became evident:

- **Alert Overload and Fatigue:** Analysts faced thousands of low-fidelity alerts and repetitive triage tasks each day, leading to alert fatigue and slower responses. In a crisis (like a multi-stage exchange breach), critical warning signs can be lost in the noise.
- **Siloed, Manual Processes:** Piecing together an attack required manually correlating data across disparate tools (SIEM logs, blockchain monitors, cloud consoles). Traditional workflows are often disjointed and static, unable to adapt when attackers pivot or use new tactics.
- **Reactive Posture:** Most SOCs remained reactive, investigating incidents only after damage was done. With threats in crypto moving at the speed of software – or even automated bots – purely reactive defenses were too slow. The Bybit hack's 20-day silent infiltration is a case in point: by the time an alert fired, the funds and evidence were gone.
- **Human Limitations:** Skilled investigators are finite, and they can be tricked. Social engineering exploits human trust, as seen in the $91M phishing scam, which no firewall or antivirus would catch. Insiders can be corrupted. Knowledge also walks out the door with turnover, causing loss of institutional memory that hampers incident response.

Adding more rules or personnel only went so far – attackers simply found the gaps, even using AI themselves to increase attack volume and sophistication. Clearly, a different approach was needed to turn the tables.

AI Agents: A New Ally for Detection, Triage, and Response

In 2025, forward-looking organizations began augmenting their SOCs with autonomous AI agents – essentially tireless virtual analysts that monitor, learn, and act at machine speed. Unlike basic automation scripts or "co-pilot" chatbots that still need constant prompting, these AI agents operate with goal-driven autonomy. Their impact on detection, triage, and response has been transformative:

- **Early Detection of Anomalies:** AI agents excel at spotting subtle patterns across huge datasets that humans might miss. In an AI-driven SOC, multiple agents continuously hunt for anomalies and correlate signals across on-chain transactions, cloud activity, and network logs. For example, an agent could flag the unusual sequence of events in the Bybit attack – a developer downloading an off-pattern update, a sudden privilege escalation, and an out-of-band code change – long before the final theft occurred. In the DeFi realm, AI models can be trained on smart contract behavior to recognize suspicious transactions or logic calls and alert on potential exploits within seconds, possibly fast enough to freeze funds. This

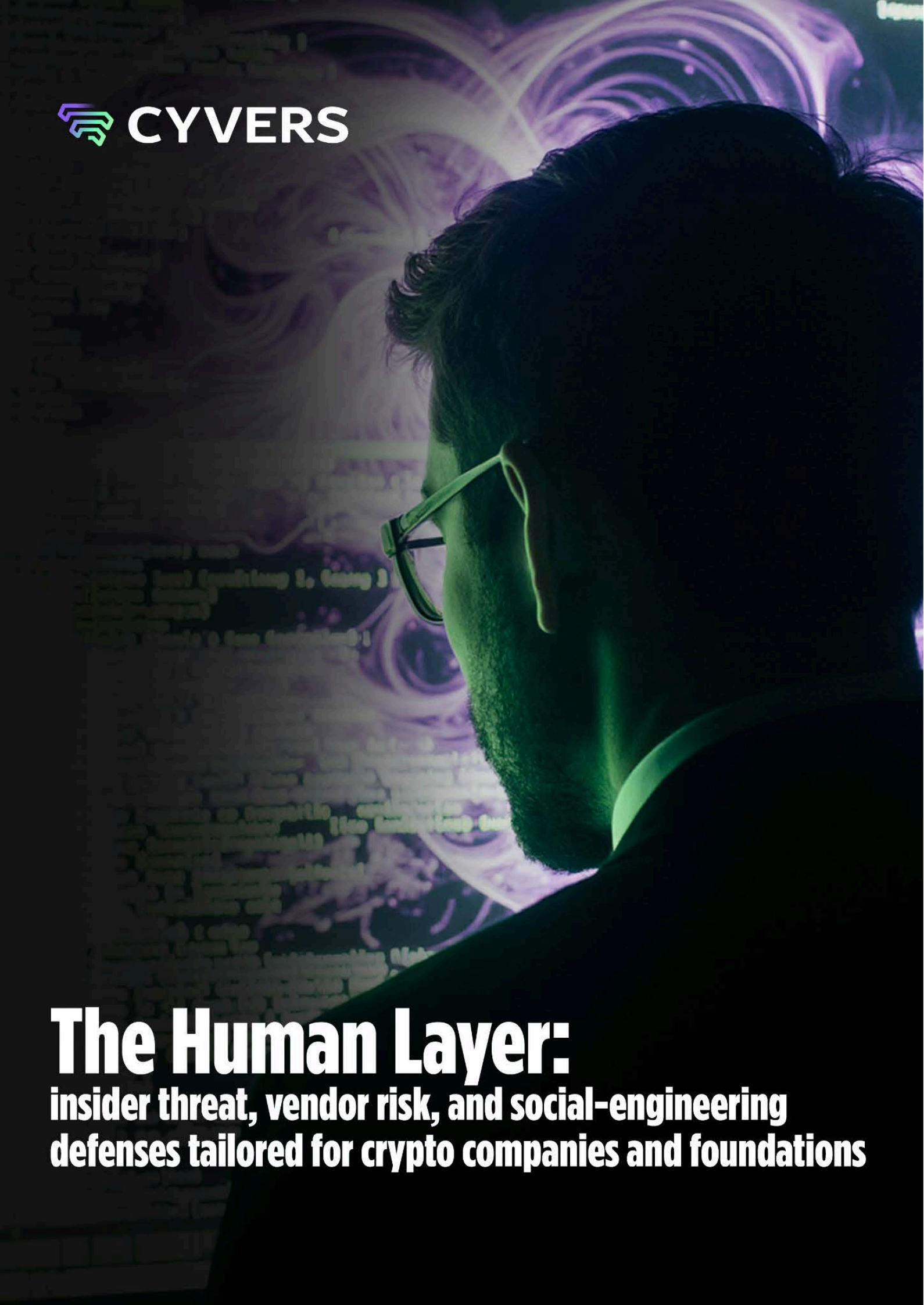
proactive monitoring contrasts sharply with static rule-based alerts, and it catches threats earlier by reducing time to action.

- **Autonomous Triage and Noise Reduction:** A major benefit of AI SOC agents is cutting through the noise. Rather than inundating analysts with every minor alert, agents can filter out false positives, cluster related events, and prioritize the truly critical incidents without human intervention. This was crucial in 2025's high-scam environment – AI-driven systems could analyze user behavior and communication content to weed out the countless scam messages and only escalate genuine pig-butchering ring indicators. The result is a drastic reduction in alert volume. Top AI-enhanced SOC platforms report they reduced false positives by up to 80% and significantly eased analyst workloads. In practice, that means when a real attack hits – like a phishing attempt against an executive or an anomalous transfer from a cold wallet – the SOC isn't too busy to notice. AI handles the mundane, so humans can focus on high-impact judgments.
- **Speedy, Orchestrated Response:** When a threat is confirmed, AI agents can also take action (with appropriate oversight). They can enrich incidents with context, trigger predefined containment of playbooks, or even initiate responses autonomously for routine cases. This agility proved vital against fast-moving attackers. Consider the rapid laundering after the Bybit hack – an AI agent integrated with an exchange treasury system might have automatically halted large suspicious withdrawals or changed API keys at the first sign of compromise, potentially limiting the haul. Similarly, in the Coinbase insider breach, an AI system monitoring employee activities might have detected anomalous access patterns and locked down those accounts before massive damage was done. Case studies indicate that AI-augmented SOCs have cut median response times by 40–60% compared to purely manual teams. Faster containment means less money lost and less time for attackers to cover their tracks.
- **Adaptation and Learning:** Crucially, AI SOC agents learn and improve over time. They ingest feedback from each incident – adjusting thresholds, updating models, and remembering new attacker techniques. This continuous learning addresses the evolving nature of Web3 threats. For instance, when scammers began using deepfake profiles or AI-generated messages in pig-butchering, advanced agents could be retrained to recognize AI speech patterns or improbable investment returns. Traditional SOC tools, in contrast, would require tedious new rules for each variant. Over 2025, the best AI-driven platforms built a knowledge base of crypto-specific threat indicators, from unusual smart contract function calls to known Lazarus Group tactics, enabling them to recognize and respond to those scenarios far quicker than any human team. As one security researcher put it, the question is no longer whether to adopt AI in the SOC, but how intelligently to do it.

A Stronger Defense for Web3

The dramatic incidents of 2025 made one thing clear: the complexity and scale of Web3 threats have outgrown human-only security operations. AI agent-powered SOCs offer a path forward. They bring the ability to watch all corners of an organization's digital estate continuously, never tiring, never forgetting, and reacting in milliseconds. This isn't to say humans are obsolete – on the contrary, the most effective model is collaboration. AI handles the heavy lifting of data analysis and first-line decisions, while skilled analysts oversee and tackle the nuanced problems. With alert fatigue diminished and routine tasks automated, human experts can apply their intuition and creativity where it matters most.

By late 2025, early adopters of AI SOCs were already reaping measurable benefits: fewer missed alerts, faster containment, and resilient operations even amid relentless attacks. In contrast, organizations sticking to traditional approaches continued to face damaging breaches and scams. The lesson from 2025 is compelling – in an arms race where hackers are using ever more advanced tools (including AI), defenders must respond with advanced AI of their own. AI agent-powered SOCs transform security from a reactive slog to a proactive hunt, fundamentally enhancing an organization's ability to safeguard the rapidly evolving world of Web3



CYVERS

The Human Layer:

insider threat, vendor risk, and social-engineering defenses tailored for crypto companies and foundations

The Human Layer: insider threat, vendor risk, and social-engineering defenses tailored for crypto companies and foundations

Executive brief

2025 has been a year of people problems at scale: a record setting exchange theft during a routine wallet operation, a major exchange reporting bribed support agents and user data exposure, deepfake enabled wire attempts in multiple regions, and a JavaScript supply chain alert affecting popular packages used in wallet apps. The data lines up with the anecdotes: the human element remains involved in roughly 60 percent of breaches, and third party involvement doubled to 30 percent year over year.

What has changed in 2025

Bigger single points of failure became common knowledge: The Bybit theft, at about 1.5 billion dollars, highlighted how routine treasury actions can spiral without strong approval and runtime checks. U.S. authorities attributed it to DPRK operators within days.

Insider enablement moved from rumor to filings: A leading U.S. exchange disclosed that external support agents were bribed, exposed data for a slice of customers, and attempted to extort the firm, with potential costs in the hundreds of millions.

Supply chain alerts touched wallet user journeys: In September, Ledger's CTO warned that malicious npm packages with over one billion downloads attempted address swapping, a classic social engineering multiplier because users approve what they think they see.

Deepfakes left the lab and hit finance desks: Singapore based cases show live video impersonation of executives to push urgent transfers, while surveys and reporting point to sharp growth in attempted deepfake fraud against enterprises.

The 2025 human-layer threat model

- **Insider threat:** privilege abuse and social or financial coercion of staff, especially at support desks and operations centers, with credential reuse and leaked secrets that linger for months. The 2025 Verizon DBIR notes the human element near 60 percent, and third party involvement at 30 percent with a median 94 days to remediate leaked GitHub secrets.
- **Vendor and supply chain risk:** poisoned SDKs, package hijacks, and CI tampering that convert UI trust into on-chain loss through payload or address swaps. 2025 npm warnings are a live example that targets the crypto stack.
- **Social engineering at speed:** deepfake Zooms and voice clones, AiTM phishing, and community impersonation that route victims to malicious approvals or urgent wires. Enterprises reported rising exposure and material losses from these tactics in 2025.

Controls that work in crypto programs, 2025 edition

The goal is simple: give people context at the exact moment value moves, reduce trust in screenshots and chats, and add circuit breakers around vendors and high-risk actions. The practices below map what leading teams shipped in 2025.

1) Pre-execution transaction simulation with policy-aware co-signing
Intercept every outbound payload before any signature, simulate effects, compare balance deltas and contract state changes, score counterparties for sanctions and scam exposure, then auto block or require step-up controls when risk crosses thresholds. This control would have reduced blast radius in warm-wallet movements like the Bybit event, and it directly counters address swap supply chain attempts because what is simulated is what will settle.

2) Dynamic, multi-hop risk scoring across chains
Replace single hop screening with real time tracing that follows funds and relationships across chains and tokens. Feed scores into approvals, treasury policies, on and off ramps, and exchange withdrawal gates. This is the practical way to catch flows tied to sanctioned actors and large scam clusters that are active in 2025.

3) Human centric identity and privileged workflows
Move administrators and signers to phishing resistant authentication, add just in time elevation, and break duties across listing, treasury, and upgrade paths. For any instruction that touches funds or keys, require two channel verification and enforce cool-downs or timelocks.

4) Social engineering defenses tuned for finance desks
Adopt live identity challenges for video calls, for example shared passphrases, gesture prompts, or handwritten tokens, pair with caller-verified backchannels, and block payment or signing requests that do not pass these checks. 2025 reporting shows these low-tech challenges expose high tech deepfakes.

5) Vendor integrity as a product requirement
Pin and sign packages, require provenance for wallet facing code, monitor registries for known bad dependencies, and route all wallet connect prompts through an approval portal that renders human readable simulations. The September npm alert is the current reminder to codify these gates.

6) Automated investigations with human in the loop
Use AI assistants that can screen counterparties, trace cross-chain flows, generate watchlists, summarize alerts, and draft regulator ready artifacts, while every action remains auditable and bound to least privilege. This directly shortens the time to freeze illicit flows that law enforcement and industry have been targeting in 2025.

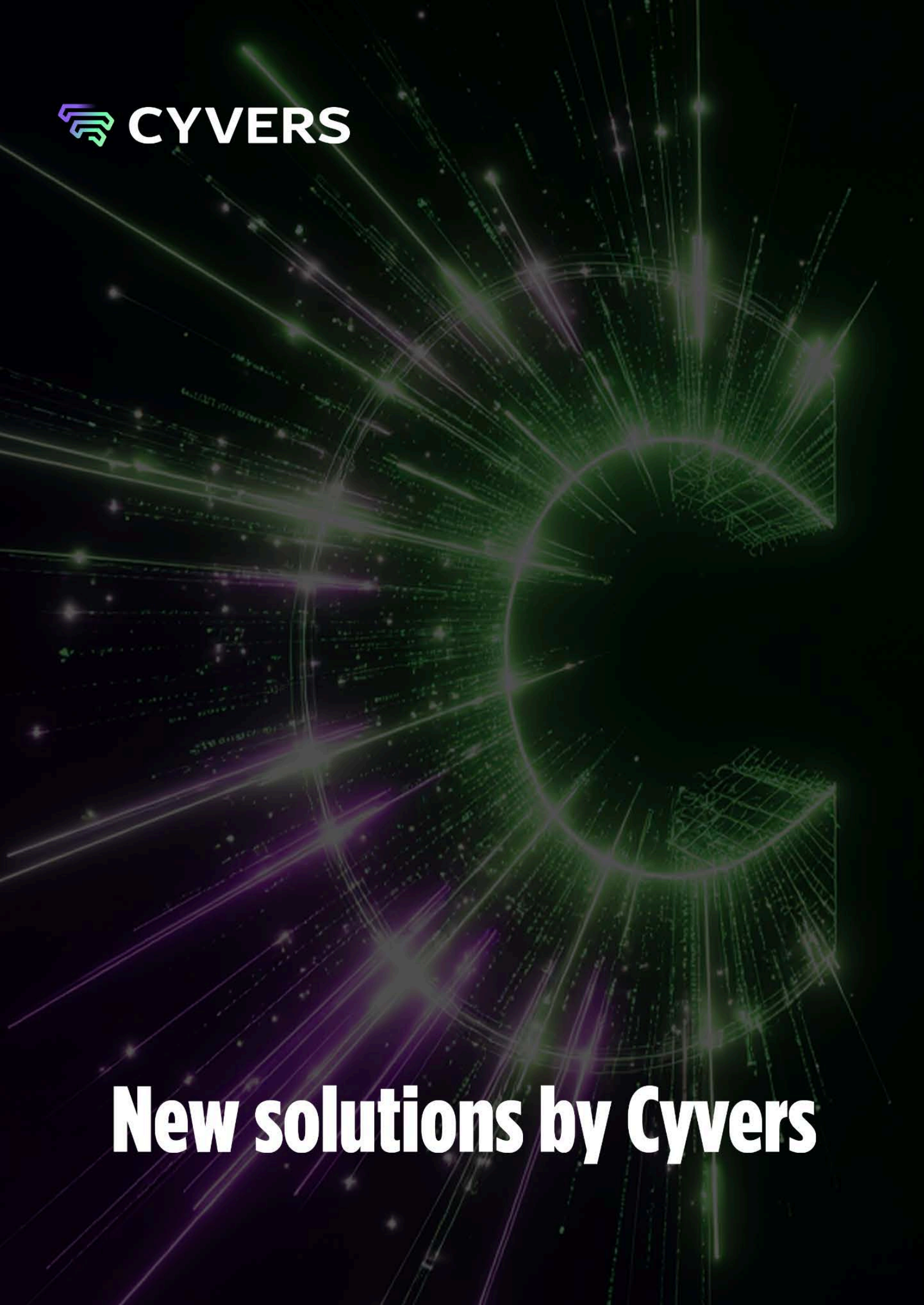
First hour playbook for 2025 incidents

- **Detect and decide:** auto simulate and score the suspicious transaction, place an immediate hold or block, snapshot evidence, and page treasury, security, legal, and comms.
- **Contain:** freeze hot wallets or counterparties under policy, add deny and allow lists, raise withdrawal friction, warn at deposit and withdrawal screens, coordinate with venues for freezes.
- **Trace and notify:** run multi hop tracing for outflows and inflows, identify cash out venues, notify bridges, issuers, and partners, and prepare packages that match law enforcement intake fields.
- **Recover and learn:** rotate keys, invalidate sessions, patch dependencies, and run a blameless postmortem that updates simulators, policies, and training.

Metrics for executives and boards in 2025

Track time to detect, time to freeze, pre-signature block rate, percent of flows auto-blocked, false positive rate at approvals, number of dependencies covered by integrity checks, and employee deepfake challenge pass rates. Align these to quarterly reviews and leadership incentives. Remember that 60% human involvement and 30 percent third party figure are the north stars for risk reduction.

Bottom line: people, vendors, and processes define crypto resilience in 2025. Programs that combine pre-execution simulation and policy aware co-signing, dynamic risk scoring, verified workflows, and vendor integrity controls are the ones that stop human layer attacks at the exact moment they matter.


CYVERS
New solutions by Cyvers

New solutions by Cyvers

Secure Co-Signing for Wallets

The Problem: wallets as the last mile of risk

Even hardened stacks, multi-sig, MPC, hardware keys, and whitelists, still fail when signers lack context at the moment of approval. In 2025, wallet breaches remain the dominant loss driver, with high profile drainers tied to blind signing, malware that tampers with payloads, and policy gaps. Real world incidents illustrate the pattern: WazirX at $235M, Radiant Capital at $50M, and the Bybit exploit in 2025 at an estimated $1.5B, not because keys or custody frameworks were absent, but because threat aware checks were not applied at runtime.

Cyvers's Solution

Cyvers acts as an intelligent co-signer embedded directly in your MPC or multi-sig flow, intercepting every transaction before the signature is finalized. The system simulates the payload against real time threat intelligence, then applies behavioral and contextual analysis, balance deltas, contract state diffs, known malicious counterparties, policy violations, and blind signing patterns. Only clean transactions are co-signed, risky ones are blocked, so prevention happens before any value moves on chain. The co-signer is designed for production use, sub second responses, compatibility with platforms like Fireblocks, Gnosis Safe, and Ledger Enterprise, and scale measured in millions of simulations each month.

What this changes in practice

Blind signing is stopped, sanctions and policy checks are enforced at the transaction boundary, and operations teams gain a deterministic veto that removes pressure from human signers. Custodians can attest to integrity at runtime, exchanges reduce manual signer risk without added friction, and compliance officers gain confidence that every outgoing transfer was vetted against risk and rules. Case reviews suggest that similar controls would have blocked the WazirX, Radiant, and Bybit sequences at the moment of co-signing.

Cyvers Agents

The Problem: manual workflows cannot keep pace

Security, fraud, and compliance teams face a flood of alerts, sanctions checks, and investigations across chains and venues. Context switching between tools wastes minutes per decision, and answers vary by analyst. In an environment defined by multi-billion pig-butchering networks and rising regulatory expectations, teams need a faster way to understand what is going on and to explain it to stakeholders.

Cyvers's Solution

Cyvers Agents are generative AI copilots that specialize in explanation. From a natural language interface, analysts can interrogate wallets, transactions, and entities, explore links to scam rings or sanctioned actors, and walk through attack paths step by step. The Agent surfaces the most relevant on- chain evidence, clarifies technical concepts, summarizes complex flows, and answers follow up questions in context.

Because Agents run on the Cyvers real time platform and intelligence graph, responses are grounded in live data, consistent with existing alerts and risk scores, and fully auditable. Security teams use the Agent to unpack anomalies and suspicious contract interactions, fraud teams use it to understand how funds moved and where risk concentrates, and compliance teams use it to obtain clear narratives that support KYT, counterparty reviews, and audit responses. At every point the human remains in control of actions, while the Agent provides the connective tissue of insight and explanation.

Why it matters

Agents compress time to understanding from minutes to seconds, align teams on a single source of context, and standardize how complex cases are explained across shifts and regions. Instead of pivoting through multiple tools, analysts ask questions in plain language, refine hypotheses, and rapidly reach a defensible view of risk. The result is faster investigations, clearer communication with management and regulators, and a more convenient workspace for researchers and analysts who need depth without friction.

The Stablecoin Trust Layer

The Problem: scale, complexity, and scrutiny

Stablecoins are becoming financial plumbing for payments, DeFi, and tokenization. Forecasts point to a $1.6T market by 2030 with issuers potentially holding $1.2T in U.S. Treasuries, a scale that invites sophisticated exploits, industrialized scams, and closer supervision under regimes like the GENIUS Act. Issuers, exchanges, bridges, and custodians need a preemptive approach that spans security, fraud, and compliance across chains and use cases.

Cyvers's Solution

Cyvers provides a unified trust layer for the stablecoin stack. The platform monitors chains, wallets, contracts, and transactions in real time, flags exploits in progress, and enables immediate freezes or interventions. Fraud defenses, dynamic address risk scoring and scam detection, block bad transfers before completion. Compliance runs continuously, screening every wallet and transaction for AML, sanctions exposure, and illicit flow typologies, with multi hop tracing, automated alerts, and audit ready reports aligned to the GENIUS Act. Reported outcomes include prevention of up to 80 percent of potential losses during active incidents, identification of more than 180,000 malicious wallets in 2024, and high fidelity coverage that caught the vast majority of on chain exploits that year.

Coverage across the ecosystem

Issuers see live mint and treasury monitoring with counterparty screening, settlement chains gain network level threat visibility, bridges receive cross chain exploit tracing, wallets and custodians get hot wallet breach alerts and transaction screening, payments providers screen destination addresses at the point of initiation, centralized exchanges block scam cash outs and protect hot wallets, liquidity and yield platforms are warned about flash loan and oracle abuse, RWA programs track provenance and flows, and insurers access incident feeds for pricing and claims. Integration is delivered through APIs and intuitive dashboards, with cross ecosystem views, real time AI prevention, and combined security, fraud, and compliance insights.

Outcome

As stablecoins scale, leaders need controls that prove resilience and compliance without sacrificing velocity. Cyvers turns visibility into preemptive action and audit ready evidence, so the ecosystem can grow safely, compliantly, and with stronger user trust.

Liquidity Security for Trading Operations

The Problem: fast markets, faster risk

Liquidity providers, market makers, and crypto hedge funds are deploying size across chains and venues, yet the risk regime can flip in minutes. Pools rebalance, bridges pause, contracts upgrade, and a single compromised key or misaligned oracle can ripple through books before a desk can react. Manual checks cannot keep pace with this surface area. What teams need is liquidity security that turns real-time onchain signals into pre-trade policy, continuous monitoring, and automated responses, so PnL is preserved, routes are protected, and operations stay steady when markets accelerate.

Cyvers's Solution: liquidity security

Liquidity security delivers real-time intelligence that protects trading operations, wallets, validators, and flows, so teams can route size with confidence while reducing slippage, operational risk, and downtime. In practice, this includes continuous monitoring of portfolio addresses and key counterparties, pre-trade reputation checks on addresses and contracts, anomaly detection on validators and hot wallets, and multi-chain screening that can automatically block or reroute transactions when risk crosses defined thresholds. The result is fewer unpleasant surprises during volatile markets, plus clear evidence trails for ops and compliance reviews.

The liquidity security stack

Pre-transaction checks and policy gates

Before significant outflows or interactions with a new contract, the system simulates intent and screens the destination. When predicted impact or counterparty risk exceeds tolerance, it requires additional approvals or blocks the flow. Safe routes pass without friction, and every decision is logged for audit and post-trade analysis.

Address, contract, and venue watch

Own wallets and the entities you interact with are observed continuously for signals like approvals to fresh contracts, unusual transfer patterns, or linkages to known threat clusters. Alerts are actionable by design, so a desk can pause a route, size down, or rotate venues within defined playbooks.

Validator and signer protection

Validators and hot wallets are monitored for performance deviations and suspicious signer behavior. If an anomaly appears, containment steps such as pausing sensitive operations or rotating keys are triggered quickly, which keeps uptime high when markets are moving fast.

Counterparty reputation scoring

Before posting liquidity or quoting size, counterparties are scored for ties to mixers, exploits, and sanctions. Scores translate directly into routing rules, spread adjustments, or collateral limits, improving fill quality while lowering exposure to clawbacks and disputes.

What proactive looks like in practice

Exploit-in-flight containment

When anomalous approvals to a fresh contract or drain-like transfer patterns appear, the receiver's reputation is flagged and policy is enforced. Risky transfers are frozen or rerouted, senior approval is required for overrides, and exposure is automatically reduced. Market makers and crypto hedge funds keep trading, while the blast radius stays contained.

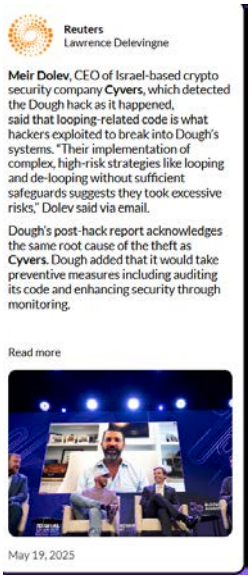
Counterparty and venue hygiene before routing size

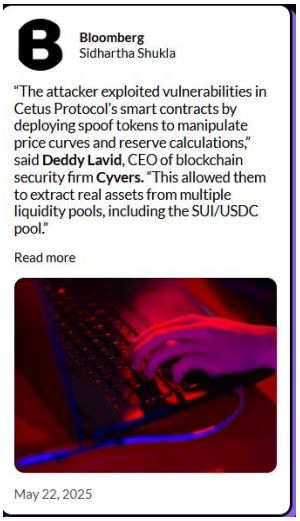
Prior to moving size, the destination's score, recent exploit proximity, and known affiliations are evaluated. High-risk routes are blocked, medium-risk flows are allowed with tighter guardrails such as smaller clips or wider spreads, and low-risk routes proceed normally. Over time, this tightens the operational loop, cuts cancellations, and supports better performance metrics.

Validator and treasury safeguard

If validator performance or signer activity diverges from normal patterns, sensitive operations are paused, keys are rotated according to playbooks, and ops is alerted for rapid recovery. This keeps downtime short and reduces emergency interventions in the middle of volatility.

Cyvers in the News





To explore further, go to [Cyvers Press & Media page](#).