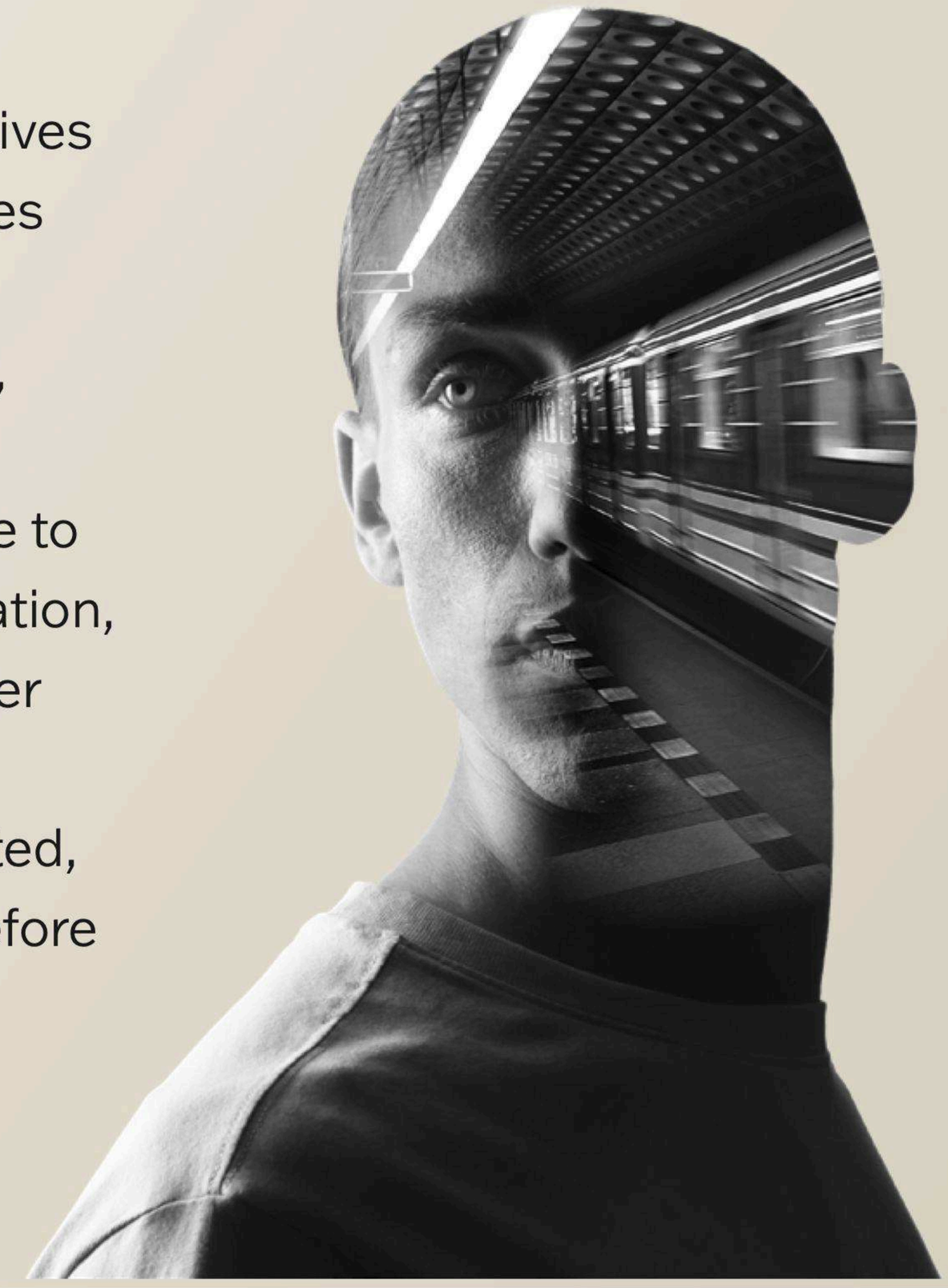
SYGNIA

The Crypto Threat Environment 2026

Understanding how crypto breaches occur and what separates organizations that contain them from those that suffer catastrophic losses.

This eBook is written for security leaders and executives in cryptocurrency businesses facing a clear shift in risk: incidents are no longer rare, and prevention alone is not enough. As attacks continue to grow in scale and sophistication, the key challenge is no longer if an incident will occur, but how quickly it can be detected, contained, and managed before impact escalates.



2025 made one thing clear for the cryptocurrency threat environment: for exchanges, custodians, DeFi platforms, and other digital asset businesses, a serious security incident is no longer a remote possibility. In Q1 2025 alone, more than $1.63 billion was lost to crypto thefts, while illicit crypto transfers over the last five years reached $189 billion[1]. These numbers reflect a threat environment where attacks are frequent, financially significant, and increasingly sophisticated.

One of the most notable examples occurred in February 2025, when nearly $1.5 billion in Ethereum was stolen from Bybit in what became the largest cryptocurrency theft recorded to date. Like many large crypto breaches, this incident was not defined[2] by a single vulnerability, but by weaknesses across access controls, infrastructure, and operational processes that ultimately allowed transaction authority to be misused.

This eBook examines how cryptocurrency security failures occur and what separates organizations that can effectively contain and recover from incidents from those where losses escalate beyond control. It focuses on where incidents begin, how transaction authority is compromised, and the architectural conditions required to prevent irreversible asset movement.

© SYGNIA 2026



THE DIFFERENCE BETWEEN TRADITIONAL FINANCE AND CRYPTO

What makes crypto incidents fundamentally different from traditional financial breaches is the structure of cryptocurrency systems themselves. Transactions are authorized through cryptographic signatures rather than institutional oversight. Once a valid transaction is confirmed on-chain, it cannot be reversed. While there are rare scenarios, such as “gas wars,” where competing transactions attempt to override one another before final confirmation, these are exceptions rather than safeguards, and do not offer a reliable mechanism for recovery.

This creates a threat environment defined by velocity and finality. In traditional finance, fraud may trigger investigation, recovery attempts, and/or legal intervention. In crypto environments, a valid signature results in immediate execution. The time between compromise and financial loss is often measured in blocks, with a dwell time of seconds or zero, rather than days.

Element	Traditional Finance	Crypto Environment	Security Implication	Operational Consequence
Trust Model Shift	Operates through institutional intermediaries, such as banks, regulators, and fraud-detection mechanisms. Transactions can be frozen, reversed, or legally contested. Example: A fraudulent wire transfer can be stopped or recalled by the bank.	Asset ownership is determined by private key control. Transactions are cryptographically validated and irreversible once confirmed on-chain. Example: Once a transaction is signed with a valid private key and confirmed on-chain, there is no institutional authority that can reverse it.	Key compromise equals asset loss.	Prevention and containment replace post-fraud recovery.

Element	Traditional Finance	Crypto Environment	Security Implication	Operational Consequence
Infrastructure & Control Complexity	Core systems are centralized and tightly governed. Access and change management are structured and predictable. Example: Even if an application server is compromised, it typically does not allow direct movement of treasury funds.	Cloud, blockchain, and application layers operate as one integrated system. Example: A privileged cloud workload or deployment pipeline can influence how transactions are generated or signed.	Privilege boundaries extend beyond infrastructure into transaction authority.	Security must protect not only systems, but transaction authority and execution paths.
Operational Tempo & Exposure	Change cycles are controlled and maintenance windows allow containment processes before financial impact occurs.	Markets operate 24/7, with deployments, upgrades, and governance actions occurring in real time.	Detection and decision windows are compressed.	Response readiness must match market velocity.

Key takeaways

- **Security must assume irreversible impact.**
  Once a transaction is signed and confirmed on-chain, it can rarely be reversed.
- **Infrastructure controls must protect transaction authority.**
  Security must safeguard not only systems, but also the pathways that influence how transactions are generated and approved.
- **Detection must operate at market speed.**
  Monitoring and response must be fast enough to identify and stop anomalous activity before assets move.

[1] CoinLaw
[2] Sygnia

© SYGNIA 2026



1. WHY CRYPTO PLATFORMS FACE DISPROPORTIONATE SECURITY RISK

Cryptocurrency businesses consolidate financial value in ways that are uncommon in traditional financial systems. Exchanges, custodians, wallets, and DeFi platforms often control large pools of digital assets designed to move quickly to support market activity and operational needs. That same speed, however, can also accelerate malicious transfers when transaction authority is compromised.

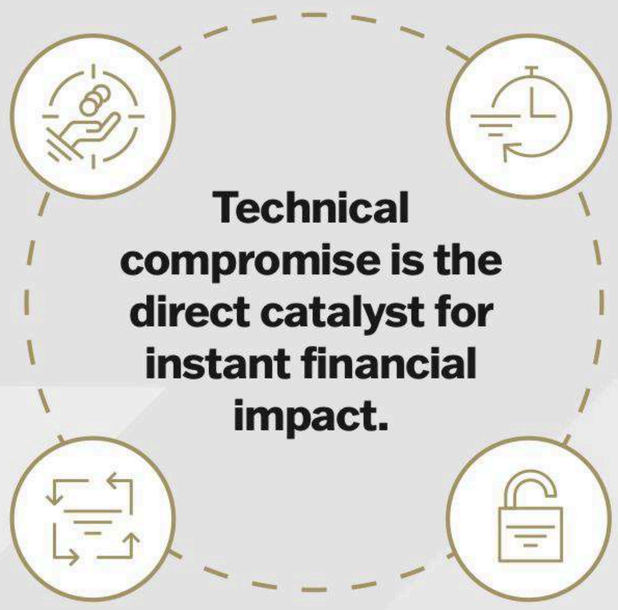
CRYPTO INFRASTRUCTURE: THE VELOCITY OF RISK

Value Concentration Creates High-Value Targets

Large asset pools are controlled by single signing mechanisms, unlike traditional finance distributed accounts.

Speed: From Breach to Total Loss

Financial impact is the immediate outcome, not a secondary consequence of investigation.



The Irreversibility of Blockchain Theft

Pseudonymity and cross-chain movement make asset recovery significantly harder than in regulated systems.

Immature Controls for Massive Treasuries

Projects often hold significant reserves without the mature operational safeguards found in traditional institutions.

Unlike traditional financial institutions, where assets are distributed across accounts, clearing systems, and regulatory controls, cryptocurrency infrastructure allows value to move directly once the appropriate credentials or signing mechanisms are accessed.

This concentration creates attractive conditions for attackers. A single compromised system, private key, or privileged identity can allow direct control over large amounts of digital assets. In many environments, infrastructure systems, cloud workloads, and transaction execution pathways are closely connected, meaning that technical compromise can translate into financial impact far more quickly than in traditional financial systems.

© SYGNIA 2026

The pseudonymous nature of blockchain networks can also complicate recovery efforts. While transactions are publicly visible, linking wallet addresses to real-world actors and recovering stolen assets can be extremely difficult, particularly once funds move across chains, through mixers, or are rapidly exchanged via decentralized platforms.

These risks extend beyond centralized exchanges. Blockchain projects, DeFi protocols, and Web3 companies frequently hold large treasury reserves in native tokens or stable assets used for liquidity, development funding, or staking rewards. These reserves can represent significant financial value, but the operational controls that protect them are often less mature than those in traditional financial environments.

In crypto environments, the financial impact of a breach is not a secondary consequence of investigation. It is often the immediate outcome of the compromise.



Organizational Impact of a Crypto Breach

When a security incident occurs in a cryptocurrency organization, the consequences unfold rapidly across multiple areas of the business. Because digital assets can move immediately once transaction authority is compromised, security events often escalate into operational and governance crises within hours.

- **Loss of user confidence**

  Even users whose funds are unaffected may initiate withdrawals after a publicized breach. This behavior can create additional liquidity pressure and accelerate reputational damage before the organization has completed its internal investigation.

- **Liquidity disruption.**

  Unauthorized asset transfers can immediately affect treasury balances and liquidity planning. Reserve allocations may no longer align with operational commitments, forcing leadership teams to reassess liquidity strategies under severe time pressure.

- **Operational disruption**

  Organizations frequently pause withdrawals, suspend trading functions, or restrict transaction flows to contain potential losses. During this period, normal business operations are deprioritized while security teams attempt to stabilize the environment.

- **Regulatory and legal escalation.**

  Security incidents can trigger notification requirements across multiple jurisdictions simultaneously. Legal teams may need to coordinate regulatory disclosures and compliance obligations before the technical root cause of the incident is fully understood.

- **Executive and governance crisis.**

  Leadership teams must make rapid decisions about disclosure, operational continuity, and financial strategy while the situation is still evolving. Board involvement often becomes immediate, with executives balancing security containment, regulatory responsibilities, and public communication at the same time.

© SYGNIA 2026



2. HOW ATTACKERS GAIN INITIAL ACCESS IN CRYPTO ENVIRONMENTS

Initial compromise frequently begins in operational environments, such as .developer workstations, source control credentials, and automation pipelines. These provide attackers with a foothold that allows them to move deeper into the infrastructure. From there, privilege escalation across cloud control planes, CI/CD systems, and runtime environments can gradually expose sensitive credentials and signing authority. Several recurring entry points appear across major incidents.

Phishing & Social Engineering Remain Primary Entry Points

Phishing and social engineering represent one of the most prevalent initial access techniques observed across cryptocurrency security incidents. Despite the technical sophistication of blockchain systems, many crypto incidents begin with human compromise. Attackers frequently launch targeted phishing campaigns aimed at developers, administrators, or employees with privileged access. These attacks often impersonate recruiters, partners, vendors, or internal colleagues to trick victims into revealing credentials or executing malicious files.

Cryptocurrency platforms are typically operated by small, specialized teams where a single individual often holds significant administrative authority across multiple systems. This means that compromising one person can be sufficient to obtain authentication tokens, private keys, or custody credentials with direct influence over transaction execution, collapsing what in traditional financial environments would require breaching multiple layers of personnel and controls into a single point of failure.

Social engineering tactics continuously evolve. Homoglyph domain attacks, malicious job offers, and increasingly convincing impersonation attempts, including deepfake audio or video, are being used to bypass traditional security awareness defenses.

Malware and Supply Chain Exploitation

Alongside phishing, supply chain compromise ranks among the most prevalent initial access techniques observed across cryptocurrency security incidents. Attackers infiltrate trusted software updates, third-party dependencies, and development tooling to introduce specialized malware into environments that would otherwise be difficult to breach directly — corrupting the tools and pipelines that developers inherently trust rather than attacking the organization head-on.

Once inside, malware operates across multiple vectors: capturing wallet credentials, authentication tokens, and development keys; monitoring clipboard activity; intercepting authentication sessions; or logging keystrokes at the point of use. Malicious browser extensions and infected development environments follow the same pattern, embedding credential-stealing capability within tools that sit at the heart of daily engineering operations.

In some cases, exploitation extends beyond the infrastructure layer to the protocol itself — vulnerabilities in smart contract code or blockchain infrastructure can be manipulated to drain assets directly, and several high-profile DeFi breaches have resulted from weaknesses in contract design or insufficient pre-deployment security testing.

© SYGNIA 2026

Human Risk and Insider Access

Insider threats represent one of the most direct pathways to asset compromise in cryptocurrency environments. Individuals with legitimate system privileges may intentionally misuse their access — as demonstrated by the 2022–2023 Coinbase insider trading case[3], in which a product manager leaked confidential token listing information to enable illicit trading profits ahead of public announcements, marking the first criminal insider trading prosecution in cryptocurrency markets.

In other cases, attackers compromise internal accounts to gain administrative control, as seen in the 2019 Bithumb breach[4], where approximately $20 million in digital assets were stolen in an incident linked to insider involvement, and the 2025 Coinbase contractor breach[5], where unauthorized access to customer KYC data was traced to a rogue service representative.

A distinct and rapidly escalating dimension of this threat is physical coercion. Physical attacks aimed at stealing cryptocurrencies, known as “wrench attacks,” jumped 75% in 2025, with 72 confirmed incidents worldwide and losses exceeding $40 million[6]. These attacks — involving kidnappings, home invasions, and targeted personal threats — are also likely underreported, with experts warning the trend will continue to accelerate[7]. The underlying logic is straightforward: as technical defenses mature, compromising the person holding the keys becomes more attractive than compromising the systems themselves.

Because privileged identities often influence infrastructure management, transaction approval processes, or custody integrations, abuse of these permissions can directly affect asset movement. Threat actors frequently conduct extensive reconnaissance before launching an attack. Public information about employees, development teams, and internal projects can help attackers craft highly targeted social engineering campaigns designed to obtain privileged access.

Complex Technology Stacks Increase the Attack Surface

Cryptocurrency platforms operate across a highly interconnected technology stack — blockchain nodes, wallet systems, cloud infrastructure, APIs, smart contracts, and identity platforms all interact to support transaction execution. New protocols, governance mechanisms, and transaction models emerge continuously, often faster than security practices can mature around them.

This architectural complexity directly translates into attack surface. Misconfigurations across distributed cloud environments, node infrastructure, and API layers are difficult to identify and govern consistently at scale. Unpatched or outdated components (across wallet software, smart contract dependencies, and underlying infrastructure) introduce known vulnerabilities that threat actors actively target.

In environments where the stack evolves rapidly and operational precedent is limited, maintaining configuration integrity and patch cadence across every layer becomes a persistent challenge that attackers systematically exploit.

Low Security Maturity and Organizational Culture

The cryptocurrency sector’s relative immaturity, combined with vendor pressure to rapidly deploy applicative features, frequently comes at the expense of securing both client-facing applications and back-office dev and ops environments. Security controls that would be considered baseline in more established industries are often deprioritized or inconsistently implemented — not due to regulatory gaps, but because security has yet to be embedded as a core organizational priority across much of the industry.

[3] U.S. Attorney’s Office, Southern District of New York
[4] The Hacker News
[5] Milberg
[6] CoinDesk
[7] DLNews



3. THE ESCALATION PATH OF A CRYPTO ATTACK

In cryptocurrency environments, initial access often occurs through conventional techniques such as phishing, software exploits, or supply chain compromise. What distinguishes these incidents is where the attack ultimately leads. Successful compromises consistently culminate in the same objective: control over transaction-signing authority. Attackers escalate privileges methodically — moving from developer workstations and automation pipelines through cloud control planes and CI/CD systems — until they reach the infrastructure responsible for generating, approving, or broadcasting transactions.

By the time attackers reach wallet infrastructure or custody authorization layers, the critical path has often already been established. The systems responsible for generating, approving, or signing transactions become accessible because earlier layers in the environment allowed privilege expansion without sufficient restriction.

ANATOMY OF A CRYPTO INCIDENT

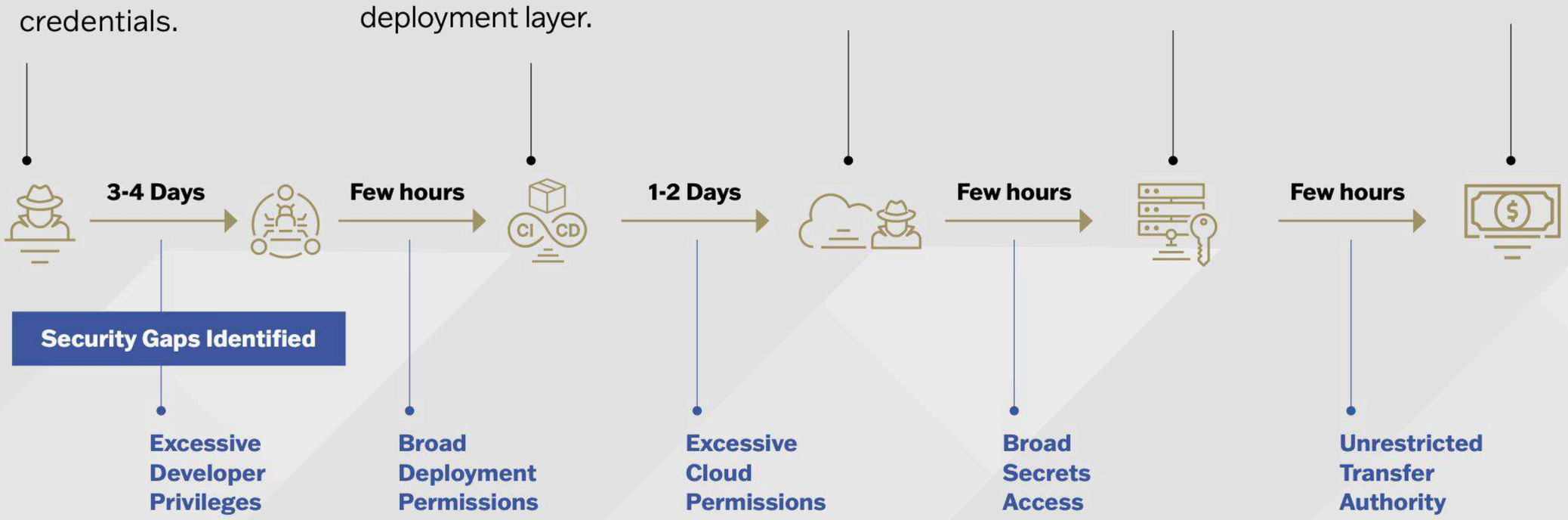
Developer Surface Compromise
Initial access is obtained through a workstation, development environment, or source control credentials.

CI/CD & Automation Identity Abuse
Pipeline tokens or service identities are leveraged to expand access within the deployment layer.

Cloud Control Plane Escalation
IAM roles or cloud permissions are exploited to gain broader administrative capability.

Runtime & Secrets Access
Kubernetes workloads or runtime privileges are used to retrieve sensitive credentials from key stores.

Wallet / Custody Authorization Reach
Access extends to signing infrastructure or custody APIs capable of initiating asset transfers.



The result is predictable progression: operational access evolves into infrastructure control, infrastructure control exposes secrets, and secrets provide the authority required to initiate asset transfers.

© SYGNIA 2026

Common Failure Patterns in Crypto Environments

> Unclear asset control and centralized authority

In many environments, it is not clearly defined where transaction authority ultimately resides. Private wallet keys may exist in signing environments with unclear ownership, multi-party computation (MPC) or hardware security module (HSM) infrastructure may be accessible through multiple administrative paths, and custody API credentials may be embedded directly in application services. In practice, the API layer in front of a custody provider often becomes the true transaction control point, yet it is rarely treated as a crown-jewel asset requiring heightened protection.

> Policy without enforcement

Security policies may define how transactions should be approved or restricted, but the architecture does not technically enforce those rules. Examples include manual approval processes for large withdrawals without system-enforced limits, two-person authorization policies without true technical separation, or destination allowlists that exist internally but are not enforced in custody systems. When policy is not embedded into infrastructure controls, governance processes can be bypassed once privileged access is obtained.

> Fragmented visibility and reactive detection

Monitoring systems often operate in isolation, leaving security teams without a unified view of activity across infrastructure, identity systems, and blockchain transactions. On-chain activity may be monitored separately from IAM and infrastructure telemetry, behavioral baselines for transaction patterns may not exist, and organizations may lack the authority or technical capability to suspend custody credentials immediately. In crypto environments, blockchain transactions can confirm within minutes while internal escalation processes take much longer, allowing financial impact to occur before response actions are taken.

© SYGNIA 2026

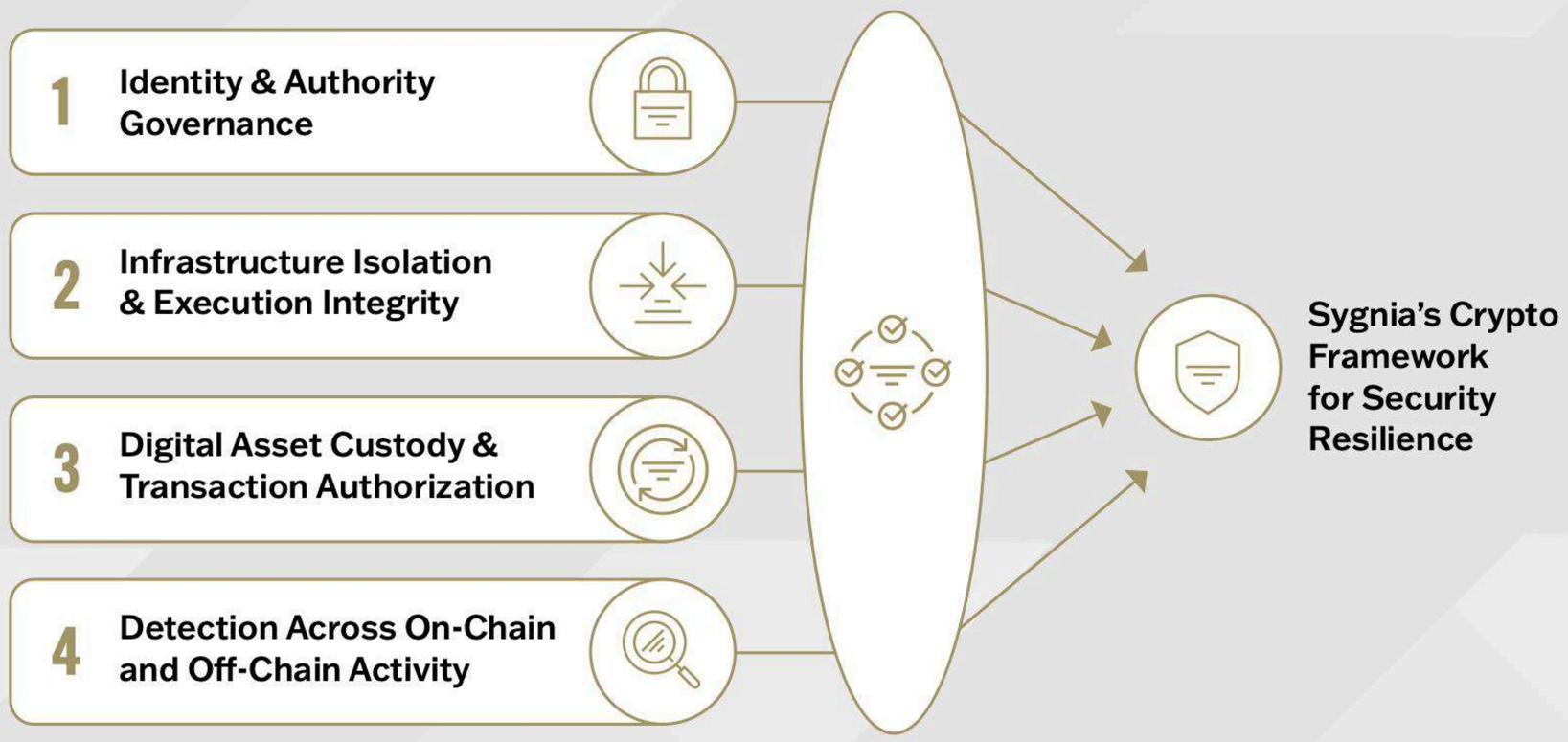
4. BUILDING SECURITY RESILIENCE IN CRYPTO ORGANIZATIONS

Resilient cryptocurrency security emerges from a coordinated system of safeguards that collectively protect transaction authority — and where prevention fails, enable rapid detection and containment before irreversible asset movement occurs. Digital asset environments combine infrastructure, identity systems, custody mechanisms, and blockchain operations into a single operational stack. Weakness in any one of these layers can create a pathway to asset movement.

For this reason, crypto security must be evaluated as a set of interdependent control domains rather than a collection of individual protections.

4 CORE SECURITY DOMAINS FOR SAFEGUARDING DIGITAL ASSET CONTROL

The sum is better than its parts



When these domains are aligned, organizations can prevent small operational compromises from escalating into financial incidents. When they are misaligned, systemic weaknesses emerge, allowing attackers to gradually gain transaction authority.

© SYGNIA 2026

Identity and Authority Governance

In cryptocurrency environments, privileged identities can directly influence transaction authorization and governance decisions. As a result, misuse of authority is often a control failure rather than a purely technical exploit. Effective security requires explicit governance over how authority is assigned, exercised, and reviewed.

- **Maintain authority mapping**

  Maintain a clear inventory of all identities capable of influencing transaction or governance decisions. This includes individuals who can approve withdrawals, modify transaction thresholds, or manage custody integrations.

- **Manage privilege lifecycle**

  Review and manage access rights alongside business roles. When personnel change responsibilities, reassess and adjust privileges connected to transaction systems or custody infrastructure accordingly.

- **Enforce just-in-time access**

  Minimize standing administrative privileges Temporarily grant and automatically expire elevated permissions expire after predefined time windows.

- **Segregate governance roles**

  Separate operational execution and strategic authority. For example, individuals who prepare treasury transfers cannot independently approve governance changes that modify withdrawal policies.

- **Periodically validate entitlements.**

  Regularly review privileged access to prevent accumulation over time. Remove dormant or unnecessary permissions to reduce long-term exposure.

Infrastructure Isolation and Execution Integrity

In crypto environments, infrastructure forms part of the transaction execution chain. Systems responsible for generating, approving, or broadcasting transactions cannot be treated as ordinary IT workloads. Infrastructure must therefore be engineered to prevent indirect influence over value execution.

- **Segment execution environments segmented**

  Isolate systems responsible for transaction processing from general infrastructure workloads. Operate blockchain nodes, operational services, and deployment pipelines in technically separated environments.

- **Control privileged access.**

  Tightly restrict, time-bound and continuously monitor administrative access to production environments and signing infrastructure.

- **Enforce deployment integrity**

  Require formal review and integrity validation of Code changes affecting transaction logic, custody integrations, or governance parameters before release.

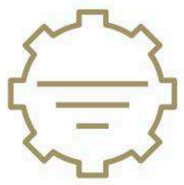
- **Ensure secrets are non-extractable**

  Store sensitive credentials such as private keys or custody API tokens in hardened environments that prevent raw export or duplication.

- **Protect telemetry.**

  Centrally aggregate and store security-relevant system in tamper-resistant environments to preserve forensic reliability.

© SYGNIA 2026



Digital Asset Custody and Transaction Authorization

The core objective of crypto security architecture is to protect transaction authority. Resilient organizations design custody systems to prevent any single pathway from independently executing asset transfers.

> **Clearly define asset control**

Formally identify where transaction authority resides. This may include internally managed signing keys, MPC infrastructure, or API credentials used to instruct third-party custodians.

> **Enforce authority separation**

Distribute transaction initiation, review, and execution functions across technically independent control points.

> **Harden authorization layers**

Isolate signing infrastructure and custody integrations from standard application workloads and protect through strict access governance.

> **Embed transaction controls**

Implement risk controls such as transfer limits, destination restrictions, and approval thresholds directly in system logic rather than relying on manual policy enforcement.

> **Ready containment mechanisms**

Immediately suspend transaction capabilities when anomalous behavior is detected.



Detection Across On-Chain and Off-Chain Activity

Monitoring in cryptocurrency environments must extend beyond traditional infrastructure telemetry. Effective detection requires simultaneous visibility across blockchain activity, infrastructure systems, and identity behavior. Security teams must be able to correlate these signals to identify deviations before asset transfers occur.

> **Establish unified monitoring**

Correlate blockchain activity with infrastructure telemetry and identity signals to provide contextual visibility into transaction behavior.

> **Define behavioral baselines**

Establish expected patterns for withdrawal volumes, destination clusters, and transaction timing.

> **Monitor governance changes**

Ensure adjustments to custody parameters, approval thresholds, or transaction policies generate immediate alerts.

> **Enable real-time alerting**

Detect high-risk activity at the moment of transaction initiation, not after confirmation.

> **Link detection to restriction**

Link monitoring to automated controls that can suspend transactions or restrict withdrawal capabilities.

© SYGNIA 2026



5. DETECTING CRYPTO INCIDENTS BEFORE FUNDS ARE TRANSFERRED

In cryptocurrency environments, the window between compromise and financial loss can be extremely short. Once attackers gain influence over transaction authority, asset transfers can occur within minutes. For this reason, detection capabilities must focus not only on identifying compromise but on recognizing signals before unauthorized transactions are executed.

Effective detection requires visibility across both blockchain activity and the systems that influence transaction execution. Organizations that successfully identify incidents early typically combine infrastructure monitoring, behavioral analytics, and blockchain telemetry into a unified detection strategy.

Complete Visibility Across the Crypto Stack

Visibility in cryptocurrency environments extends far beyond traditional infrastructure monitoring. Security teams must maintain continuous insight across both on-chain and off-chain components that influence asset movement. This requires telemetry and observability across multiple layers, including:

- **On-chain transaction behavior and smart contract activity**
- **Off-chain infrastructure such as cloud services, nodes, and APIs**
- **Identity systems and private key usage**
- **Development and deployment pipelines**
- **External attack surface exposure**

Blockchain analytics platforms extend this visibility further by maintaining large databases linking wallet addresses to exchanges, ransomware groups, scam wallets, and sanctioned entities. Detection in this context involves identifying when a transaction touches high-risk counterparties and calculating exposure to illicit funds — capabilities that are native to blockchain environments and have no direct equivalent in traditional financial monitoring.

Real-Time Anomaly Detection

Early detection depends on identifying deviations from normal behavior across both technical infrastructure and blockchain activity. Security teams should instrument monitoring to correlate signals across multiple domains simultaneously and trigger alerts when the following are observed:

- **On-chain activity**

  Unusual transaction patterns, abnormal token flows, or unexpected smart contract events

- **Infrastructure behavior**

  Suspicious API calls, anomalous wallet-signing activity, and unexpected cloud operations

© SYGNIA 2026

- **Identity signals**
  Unusual authentication patterns or privileged access activity

Correlation across these domains is critical. For example, an identity anomaly combined with unusual wallet-signing activity carries significantly higher risk than either signal in isolation and should trigger immediate investigation, rather than just generating an automated alert.



Proactive Threat Hunting

Threat actors targeting cryptocurrency platforms often operate patiently within compromised environments before executing theft. As such, proactive threat hunting plays a critical role in identifying subtle signals of attacker activity.

Effective threat hunting combines traditional security investigation techniques with blockchain analytics and behavioral analysis of transaction systems in search of indicators such as:

- Changes in wallet behavior, such as abnormal outbound transfers, new beneficiary addresses, or sudden increases in transaction frequency
- Smart contract activity that deviates from expected usage patterns, including repeated failed transactions or unexpected function calls
- Credential or access anomalies, such as unauthorized RPC endpoint access or suspicious API activity targeting signing systems
- DeFi or bridge-related attack patterns, including oracle manipulation, flash-loan exploits, or relayer impersonation

Identifying these signals early can reveal attacker's presence before the transaction authority is abused.



Rapid Containment

Detection alone is insufficient without the ability to respond immediately. However, suspending transaction capabilities based on anomalous activity is not a decision that can be made automatically. False positives carry real business consequences, and indiscriminate containment can introduce operational friction that itself becomes disruptive.

The capability to isolate compromised systems, revoke credentials, restrict API access, or suspend transaction functions must exist and be continuously maintained. But its invocation should be deliberate, scenario-driven, and governed by predefined escalation criteria that weigh the severity and confidence of the signal against the operational impact of interruption. Organizations that have defined these thresholds in advance, rather than making them under pressure during an active incident, are significantly better positioned to act decisively when it matters.



Threat Intelligence Integration

Cryptocurrency environments demand a threat intelligence capability that extends well beyond conventional feed consumption. The public and pseudonymous nature of blockchain networks creates a uniquely rich intelligence surface — one that, when properly instrumented, allows security teams to detect malicious activity, trace stolen funds, and anticipate attacker behavior with a degree of precision unavailable in traditional financial environments.

Effective threat intelligence in this context spans several interconnected domains:

© SYGNIA 2026

- **On-chain intelligence.**

  Analysis of blockchain transactions, wallet clusters, and fund flows enables identification of malicious actors, laundering paths, and stolen-fund movements. Because ledgers are public, investigators can trace transactions and link addresses to specific entities or threat groups — turning the transparency of blockchain against the attackers who exploit it.

- **Wallet and entity attribution**

  Use of threat intelligence platforms to map blockchain addresses to exchanges, ransomware groups, mixers, sanctioned actors, and criminal organizations enables real-time risk scoring and detection of suspicious interactions before funds move beyond reach.

- **Threat-actor profiling**

  Maintain intelligence on groups with a sustained focus on cryptocurrency targets — such as the North Korean Lazarus Group — to track their techniques, infrastructure, and active campaigns, providing the context needed to identify early-stage intrusion activity before it escalates.

- **Embed transaction controls**

  Implement risk controls such as transfer limits, destination restrictions, and approval thresholds directly in system logic rather than relying on manual policy enforcement.

- **Cross-chain and laundering analysis**

  Post-breach, stolen assets move quickly across chains, bridges, mixers, and DeFi services. Threat intelligence focused on these laundering patterns allows organizations and investigators to maintain visibility into fund movement even as attackers attempt to obscure the trail.

- **Dark web and underground monitoring**

  Hacker forums, exploit markets, and leaked datasets frequently surface discussions about exchange vulnerabilities, stolen wallets, or planned attacks before they materialize. Monitor these channels for early warnings that are difficult to obtain through infrastructure telemetry alone.

- **Web3-specific attack technique intelligence**

  This includes phishing campaigns targeting private keys, smart contract exploitation, validator compromise, supply chain attacks on wallet software, and developer infiltration — the techniques most observed across high-impact cryptocurrency incidents.

- **Financial crime and sanctions intelligence**

  Tracking illicit crypto flows, sanctions evasion, and ransomware payments through blockchain analytics and regulatory intelligence feeds supports both detection and compliance obligations across jurisdictions.

Detection reduces the time attackers can operate unnoticed, but it does not eliminate risk entirely. When suspicious activity escalates into an active compromise, organizations must be prepared to respond immediately.

In crypto environments, detection is only valuable if it occurs before transaction authority is exercised.



© SYGNIA 2026

6. INCIDENT RESPONSE: LIMITING IMPACT ONCE AN ATTACK IS UNDERWAY

While incident response principles remain consistent with traditional cybersecurity practice, cryptocurrency incidents place exceptional demands on speed. Stolen assets can be transferred and laundered across blockchain networks within minutes, and transactions are generally irreversible. This means that every minute of delayed response directly translates into unrecoverable loss.

The urgency compounds further once a breach becomes public. Publicized incidents attract additional threat actors who actively monitor for signs of compromise and move quickly to exploit residual access, weakened controls, or the operational chaos of an organization under pressure. Containing the incident rapidly is therefore not only about stopping the original attacker, but also about closing the window before others attempt to exploit the same vulnerability.

Forensic Analysis

IR forensic investigations typically analyze infrastructure logs, identity activity, and blockchain transaction data to reconstruct the sequence of events. Understanding the attacker's entry point, privilege escalation path, and interaction with transaction infrastructure is essential for determining the full scope of the incident.

Rapid Response and Containment

Once malicious activity is confirmed, incident response teams must move quickly to restrict the attacker's ability to operate within the environment. This may include isolating compromised systems, revoking credentials, disabling signing capabilities, or restricting withdrawal functionality. The objective is to prevent additional asset transfers while preserving evidence needed for investigation.

In case of an incident, containment and investigation often run in parallel. Initially containing actions are taken immediately upon confirmation of malicious activity, with forensic findings continuously informing and refining the containment strategy as the incident unfolds.

© SYGNIA 2026

Remediation

After containment, organizations must restore normal operations while addressing the weaknesses that enabled the incident. This may involve patching vulnerabilities, strengthening identity and access controls, redesigning portions of infrastructure, and improving monitoring coverage. The remediation steps reduce the likelihood that the attacker will re-enter the environment or exploit the same pathway again.

Legal and Regulatory Compliance

Security incidents involving cryptocurrency platforms can trigger reporting obligations across multiple jurisdictions. In such cases, IR teams will need to document the breach, preserve forensic evidence, and coordinate with legal and regulatory stakeholders as required.

Communication Management

Communication is critical to managing a cryptocurrency security incident. Organizations must provide accurate updates to leadership, customers, regulators, and partners while the investigation is ongoing. Incident response teams can support these communications to ensure messaging remains consistent, transparent, and aligned with the evolving understanding of the incident.

© SYGNIA 2026

7. CASE STUDY: TARGETED CRYPTOCURRENCY THEFT VIA CLOUD COMPROMISE

To illustrate the severity and complexity of these threats, consider the case of CryptoCo (name changed), a cryptocurrency platform that suffered losses exceeding $12 million in digital assets to a sophisticated attack attributed to a North Korean state-sponsored threat actor.

Sygnia was engaged in 2024 to investigate unauthorized cryptocurrency transactions originating from CryptoCo Exchange, which operated its platform on AWS cloud infrastructure. The investigation revealed a multi-stage breach involving social engineering, credential theft, and cloud infrastructure compromise, eventually allowing the attacker to influence the exchange's transaction infrastructure.

$12M+ stolen

40 unauthorized transactions

5 cryptocurrencies affected

Initial access:
LinkedIn social engineering

Infrastructure:
AWS (EC2, EKS)

Additional access:
Microsoft 365 via SSO

Attack Progression

1. **Initial Access – Targeted Social Engineering**

   The attack began with a targeted social engineering campaign. A CryptoCo developer was approached on LinkedIn by a fake recruiter offering a fraudulent job opportunity. As part of the recruitment process, the developer was sent a malicious "home assignment." When the file was downloaded and executed on the developer's corporate laptop, it installed credential-stealing malware.

2. **Credential Theft – AWS Access Tokens Compromised**

   The malware extracted privileged AWS access tokens from the compromised laptop. Using these tokens, the attacker gained unauthorized access to CryptoCo's AWS environment. To ensure continued access, the attacker immediately created a new AWS access key with elevated privileges, allowing them to maintain persistence even if the original compromised credentials were rotated or detected.

3. **Establishing a Cloud Foothold**

   Using the newly created access key, the attacker established a foothold on an EC2 instance. They then deployed malware through AWS Systems Manager (SSM). This allowed them to create a backdoor communication channel to their command-and-control (C2) infrastructure without needing direct interactive access.

4. **Reconnaissance and Lateral Movement**

   Over the following days, the attacker conducted extensive reconnaissance inside the AWS environment. They mapped infrastructure components and performed lateral movement using SSH to access additional EC2 instances. Despite CryptoCo's relatively mature security posture, the attacker was able to exploit trusted relationships within the application's architecture, allowing them to expand their access across the environment.

5. **Privilege Escalation via Kubernetes**

   During reconnaissance, the attacker identified Amazon Elastic Kubernetes Service (EKS) as a key component of the platform's infrastructure. By compromising EKS, they were able to escalate privileges and gain full control over the exchange's critical infrastructure, significantly expanding their influence over operational systems.

6. **Asset Theft – Unauthorized Transaction Execution**

   With control over the relevant infrastructure, the attacker executed approximately 40 unauthorized cryptocurrency transactions. These transfers moved assets from cold wallets to hot wallets and involved five different cryptocurrencies, including Bitcoin and Ethereum. The transactions were designed to mimic legitimate application requests, which allowed them to bypass existing security thresholds and alerting systems.

7. **Detection**

   The attack remained undetected during execution. It was discovered only after CryptoCo identified discrepancies in transaction activity, triggering the investigation. The investigation also revealed that the attacker used the same stolen credentials to access CryptoCo's Microsoft 365 environment, including email and Teams messages, through single sign-on. This access potentially allowed the attacker to monitor internal communications and observe aspects of the incident response.

Containment, Remediation, and Outcome

After the breach was discovered, CryptoCo immediately took its services offline to prevent additional losses. Sygnia deployed a 24/7 incident response team to investigate the compromise and identify all affected systems across the environment.

The final phases of the incident response lifecycle (remediation, recovery, and hardening) were initiated following the completion of the investigation. As part of remediation, identified threat vectors and persistence mechanisms were eliminated, ensuring the attacker no longer had access to CryptoCo's environment. The recovery phase focused on restoring affected systems and services to normal operations, validated through post-breach monitoring to confirm no signs of re-entry or residual compromise.

To address the hardening phase, CryptoCo re-architected portions of its AWS environment based on prioritized security recommendations. This included strengthening IAM policies, tightening network segmentation, and implementing additional detective controls, reducing the attack surface and lowering the likelihood of similar incidents in the future.

© SYGNIA 2026

8. CONCLUSION

Architecture is the bottom line. When transaction authority is clearly mapped, technically separated, and protected as a crown-jewel asset, a compromised credential remains a containable incident rather than a financial catastrophe. When it is not, the path from initial access to unauthorized transfer is a matter of hours.

This starts with eliminating single-point transfer authority. If a single credential can complete a transaction independently, the architecture has already failed. Initiation and approval must be technically separated, custody API integrations must be treated as direct asset transfer authority, and no permanent privilege should exist that can execute transfers on its own. Equally, infrastructure-level privileges must never extend into transaction execution: deployment pipelines, cloud workloads, and operational systems must be structurally isolated from the paths that sign and broadcast transactions.

Governance must be built into the architecture, not managed alongside it. Treasury approval mechanisms, containment procedures, and decision authority need to be predefined and embedded as structural components rather than improvised under pressure during an active incident. And detection only reduces risk when every alert is linked to a control capable of acting on it, with transaction thresholds enforced programmatically and escalation authority established in advance.

For security leaders, the question is not whether an attacker can get in. It is whether your architecture can stop them from ever reaching your signing infrastructure.

ASSESS YOUR SECURE YOUR CRYPTO POSTURE BEFORE AN ATTACKER DOES

Sygnia has investigated some of the largest cryptocurrency breaches on record. That experience directly informs how we assess exchange architecture, simulate crypto-specific attack paths, and help organizations identify gaps in transaction authority governance before they become incident reports. Contact us to learn how we can help keep your crypto organization secure.



SYGNIA

DISCLAIMER

For full disclosure, Sygnia is collaborating with NVIDIA in a joint research and development effort to develop a novel approach for detection and response at the edge of ICS/OT networks. The MDR technology under development should facilitate hardware-based host-level detection in the upper layers of the OT network (levels 2-3.5), using a combination of hardware, software and AI technologies from NVIDIA and Sygnia, to allow performing sophisticated detection and response operations while adhering to Purdue-based network separation principles. Such technology-based solutions, once available, will have implications on several concepts outlined in this paper, specifically those in the Optimize section, allowing further enhancements in elevating network monitoring, enhancing endpoint detection and elevating infrastructure monitoring.

A TEMASEK COMPANY AND MEMBER OF THE ISTARI COLLECTIVE

TEMASEK ISTARI

24/7 INCIDENT RESPONSE COVERAGE

Suspicious of an incident? Call +1-877-686-8680 now. Learn more at www.sygnia.co