CASE

The $140M Insider Heist:

A CISO's Guide to Stopping the Next Breach

Executive Summary

In July 2025, Brazilian authorities arrested an insider at C&M Software who sold internal access credentials to attackers for just $2,700. That relatively minor bribe facilitated a major breach of Brazil's PIX payment system, resulting in unauthorized transfers totaling over 800 million Reais (approximately $140 million USD). The attackers abused legitimate access, not advanced exploits, to execute fraudulent transactions across six major banks.

This paper examines how identity-based controls, such as those provided by Kron PAM, could have prevented this breach even when valid credentials were used. According to IBM's 2024 report, organizations that rely solely on compliance-based approaches (e.g., audits and policies without technical enforcement) face 2.6x higher breach costs compared to those that adopt advanced, identity-based security controls. Effective defense requires operationalizing access governance and deploying real-time, identity-aware protections.

The Incident: PIX Insider Breach Breakdown

On July 4, 2025, João Roque, a 48-year-old IT employee at C&M Software, was arrested for selling privileged credentials used in the coordinated fraud of Brazil's PIX instant payment infrastructure. Attackers used these credentials to siphon nearly R$800 million (~$140 million USD) in just over 2 hours. One institution alone lost more than $100 million. Investigators report that over $50 million in assets have been frozen, with around $30-40 million traced to crypto laundering through over-the-counter (OTC) channels, peer-to-peer or broker-facilitated exchanges that often bypass traditional regulatory oversight.

Investigations and public reporting suggest this breach was enabled by several key gaps in identity governance and privileged access control:

- A lack of real-time session visibility
- Persistent privileged access to critical payment infrastructure
- No behavioral monitoring or session context analysis
- No step-up approvals or conditional access for high-risk transactions

Anatomy of Insider Threats in 2025

Insider threats now span the entire supply chain. Contractors, vendors, and MSPs often hold privileged access without undergoing the same rigorous controls applied to internal employees. This breach is a reminder: access is access regardless of the badge it wears.

Today's insider threats are increasingly subtle, distributed, and often enabled by legitimate credentials. Attackers are leveraging financial incentives, psychological manipulation, and external coercion to compromise individuals with system access. In environments where access is overprovisioned or poorly audited, the risks multiply.

Sophisticated threat actors also exploit identity blind spots using social engineering tactics like deepfakes, phishing, and fake executive approvals to fast-track access. Combined with insufficient behavioral baselining or contextual approval checks, the result is an enterprise attack surface that is wide open to abuse even from legitimate logins.

Ultimately, insider threats today blend human error, malicious intent, and systemic governance failures. Solving them requires more than password policies and vaults. It demands dynamic, real-time identity context, behavior analytics, and embedded enforcement at every step of the access lifecycle.

Common Gaps in Legacy Access Control:

Persistent Credentials:
Long-lived access tokens and static credentials are often reused or improperly shared, enabling unauthorized reuse.

Superficial Session Monitoring:
Many PAM tools log sessions but do not actively inspect or block high-risk commands or behaviors in real time.

No User Behavior Analytics (UBA):
Without baselining typical user behavior, even valid logins performing abnormal actions can go unnoticed.

Limited Identity Coverage:
Legacy systems often overlook cloud, SaaS, API, and service accounts, leaving critical access points ungoverned.

Lack of Contextual Approval:
High-risk or time-sensitive actions don't trigger extra scrutiny, like manager approval or step-up authentication.

Network Devices Lack Identity Enforcement:
Routers, switches, and OT systems often rely on shared or static credentials, with no visibility into who is executing commands.

Network-Centric Controls (e.g., NAC):
These validate device health but lack insight into the user's identity, intent, or session context.

Emerging Insider Techniques

Credentials for Sale on the Dark Web and Telegram:

Internal login credentials often stolen, phished, or leaked are readily available on underground forums and private Telegram groups. Prices vary, especially for verified or high-value accounts, and buyers increasingly include nation-state proxies and ransomware affiliates. (Sources: IBM, BitSight, The Cyber Express

Deepfake-Enhanced Phishing and Social Engineering:

Attackers now combine AI-generated voice and video with phishing tactics to bypass business processes. These impersonations bypass traditional controls by mimicking known approval paths such as a CFO requesting urgent payment or an engineer seeking database access. (Sources: DHS, The Guardian, Workforce Bulletin)

Compromised Third-Party Contractor Accounts:

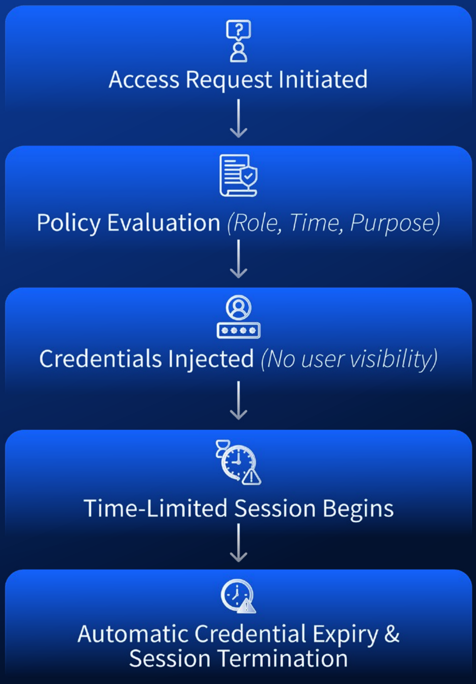
Vendors and contractors often operate with excessive privileges and limited monitoring. Their accounts are routinely targeted for takeover due to inconsistent access governance, making them ideal entry points for lateral movement or data exfiltration. (Sources: BitSight, Prey Project, Workforce Bulletin)

References & Further Reading:

- AP News
- Bitdefender Labs
- Verizon DBIR 2024: 74% of breaches involve the human element; 19% involve insiders.
- IBM Cost of a Data Breach Report 2024: Insider threats have the highest average breach cost.
- MITRE ATT&CK Insider Threat Framework: Valid account abuse and privilege escalation are now common.

EMERGING INSIDER TECHNIQUES

Workflow 1: Just-in-Time Access



Access Request Initiated

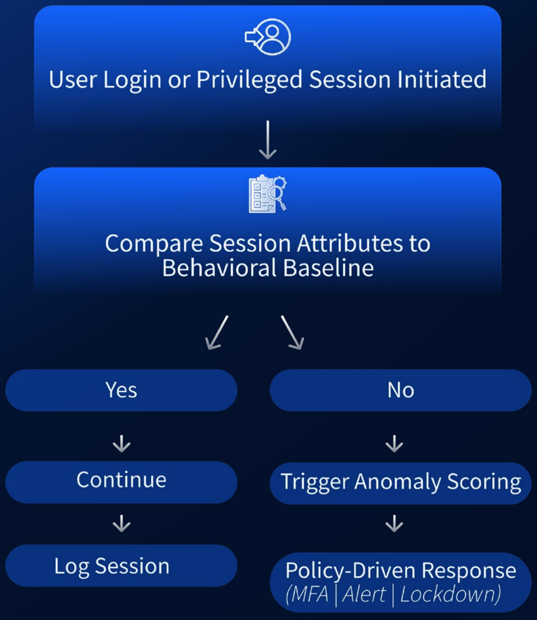
Policy Evaluation *(Role, Time, Purpose)*

Credentials Injected *(No user visibility)*

Time-Limited Session Begins

Automatic Credential Expiry & Session Termination

Workflow 2: Real-Time Behavior Analytics



User Login or Privileged Session Initiated

Compare Session Attributes to Behavioral Baseline

Yes

Continue

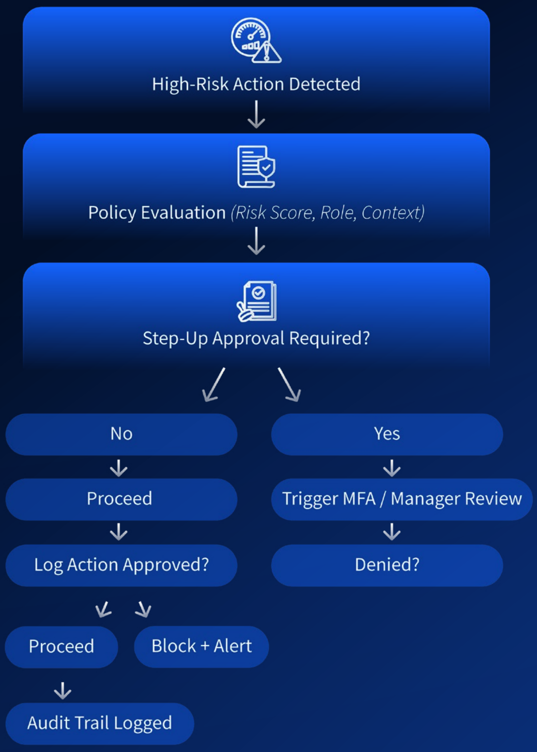
Log Session

No

Trigger Anomaly Scoring

Policy-Driven Response *(MFA | Alert | Lockdown)*

Workflow 3: Step-Up Approvals



High-Risk Action Detected

Policy Evaluation *(Risk Score, Role, Context)*

Step-Up Approval Required?

No

Proceed

Log Action Approved?

Proceed

Audit Trail Logged

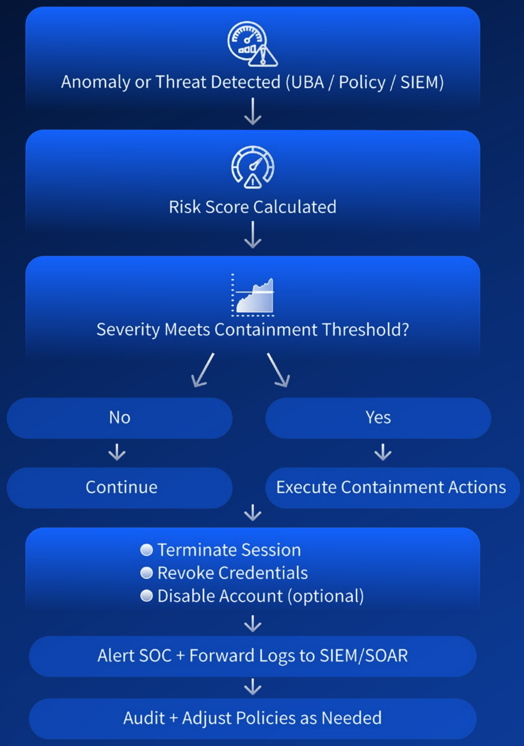
Block + Alert

Yes

Trigger MFA / Manager Review

Denied?

Workflow 4: Automated Containment



Anomaly or Threat Detected (UBA / Policy / SIEM)

Risk Score Calculated

Severity Meets Containment Threshold?

No

Continue

Yes

Execute Containment Actions

- Terminate Session
- Revoke Credentials
- Disable Account (optional)

Alert SOC + Forward Logs to SIEM/SOAR

Audit + Adjust Policies as Needed

Threat Vector	***Legacy Controls***	***Kron Identity-Based Controls***
Sold Credential	Password rotation	*Just-in-time access with no reuse*
Deepfake Approval	None	*Step-up approval with live audit trail*
Lateral Movement	Basic NAC	*Behavior-based anomaly detection*
Insider Privilege Escalation	Static roles	*Dynamic access policies + session contex*

Compliance Is Not Security

Frameworks like ISO 27001, NIST 800-53, and PCI-DSS provid e minimum baselines. But:

- A compliant system may log privileged access but not block it
- A compliant system may store credentials but not monitor live usage
- A compliant system may require MFA on login but not for critical actions

Security Leaders Must Evolve:

- Move beyond audits to real-time detection and enforcement
- Elevate session context as a first-class control signal
- Demand behavior-aware workflows in your PAM strategy

Recommendations for CISOs

1.Audit Third-Party and Internal Identity Risks

Map all external and insider access paths to critical systems.

2. Operationalize PAM for Real-Time Enforcement

Replace static vaulting with just-in-time controls and contextual approvals.

3.Shift from Compliance-Only to Continuous Access Governance

Build identity context and session awareness into every critical workflow.

Final Thought

The PIX breach is more than a regional event, it is a global signal flare. When attackers can weaponize a $2,700 bribe to steal $140 million, it's a stark reminder that technical exploits aren't the biggest threat, access is.

In today's identity-driven threat landscape, even legitimate credentials can become tools of destruction. Security leaders must ask: are we truly resilient, or simply compliant?

Is your access control just compliant or breach-resilient?