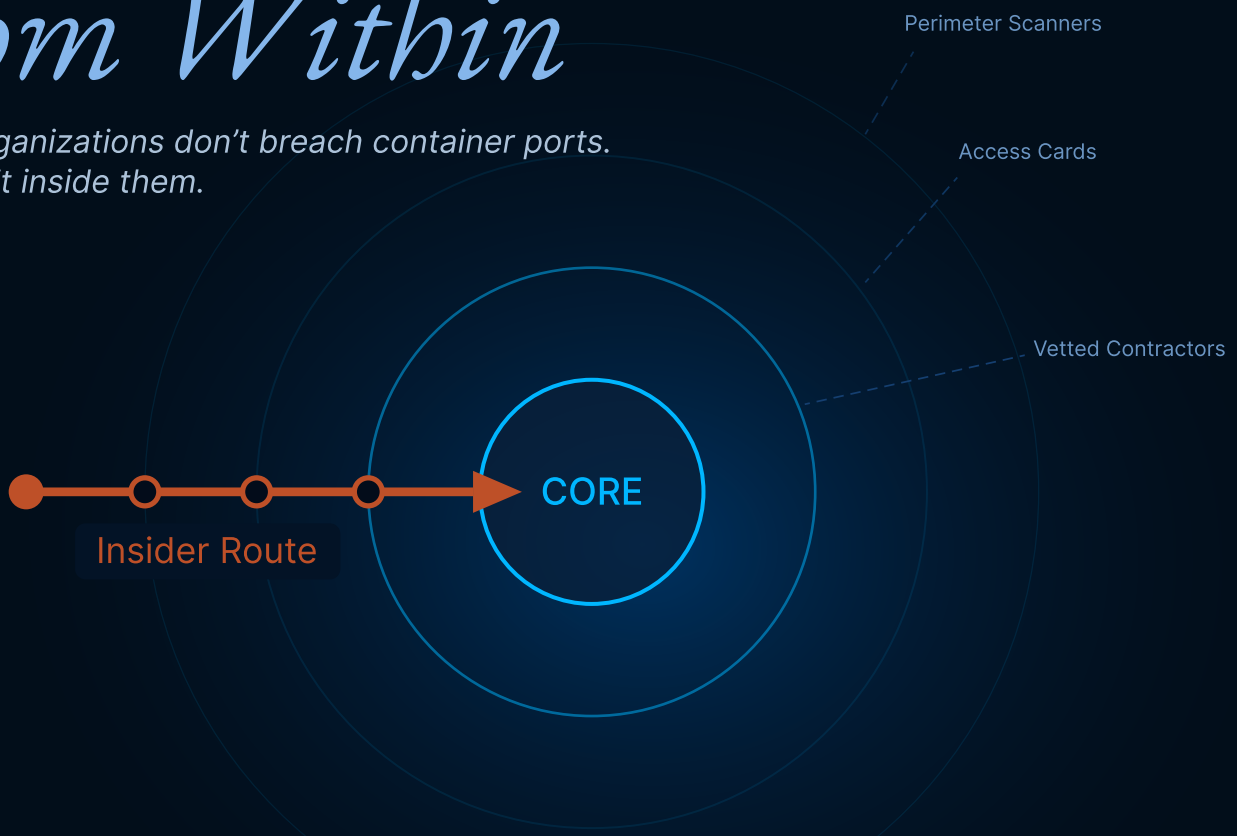
Aperia

ICM
Powered by Tapestrii

PORTS UNDER PRESSURE SERIES • May 2026

The Vulnerability *From Within*

Criminal organizations don't breach container ports. They recruit inside them.



7–20%

Cargo value paid to corrupt dock workers per facilitated shipment (Europol, 2022)

~290 MT

Cocaine seized in Ecuador in 2024, 30% above 2023 (UN INCB, 2025)

4+

Disconnected systems hold the signals; no one sees across them

THREE FAILURES. ALL INVISIBLE.

ONE-TIME VETTING

Workers cleared at hire generate no flag when recruited years later

SILOED SIGNALS

Access logs, manifest queries, and incidents live in separate systems

RETROSPECTIVE ONLY

Patterns become visible only after the seizure makes them obvious

tapestriisupport@aperia.com
www.aperia.com/platforms/tapestrii-icm

Consider a scenario assembled from documented patterns across Latin American (LATAM) terminals. A dock worker swipes into the container yard at a shift change. The credentials are valid. The access window matches the worker's assigned role. The shift handover is busy enough that the timing reads as routine. Two months later, customs in Rotterdam intercepts a container originating from that terminal with several hundred kilograms of cocaine concealed in a legitimate refrigerated shipment. The retrospective investigation pulls access logs, manifest queries, and incident records. The pattern was there. No single system had assembled it.

No breach. No intrusion. A trusted person, already inside, had become the mechanism. This is the threat that does not look like a threat, because operationally, in real time, it looks exactly like normal work. The remainder of this paper examines why that signature is so difficult to detect, and what would be required to see it before the seizure makes it visible.

The Architecture of Access

Moving cocaine at scale is not an intrusion problem. It is an access problem.

Container shipping moves more than 720 million containers globally each year, carrying roughly 90 percent of world cargo.[1] The volumes of cocaine now departing LATAM ports (hundreds of metric tons annually across Ecuador, Colombia, Brazil, and the Southern Cone) are not moved through that system by improvisation. Each shipment requires container codes, bay positions, inspection routing, seal records, and movement timing. None of that information is publicly available. All of it sits with people who work at the terminal.

Criminal networks have organized themselves around this structural reality. Insider access is not a fallback when external smuggling fails. It is the primary mechanism. In its April 2023 joint analysis with the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven, and Rotterdam, Europol designated the corruption of port personnel (dock workers, logistics and security employees, customs and law enforcement officers) as the "key enabler" for criminal infiltration of Europe's three largest ports.[2] The same dynamics now apply, with mounting evidence, to LATAM departure ports.

The economics of recruitment have escalated to match. In October 2022, an Italian Guardia di Finanza operation, supported by Europol and Eurojust, dismantled an 'Ndrangheta-linked network running cocaine through the port of Gioia Tauro. The investigation documented field coordinators paying corrupt dock workers commissions of 7 to 20 percent of cargo value per facilitated shipment, alongside a corrupt customs officer who altered the outcome of an x-

ray scan in exchange for 3 percent of the cargo value. The seized shipments totaled more than four metric tons of cocaine with an estimated street value above €800 million. [3] At those rates, a worker's share of a single facilitated shipment exceeds several years of legitimate wages. This is not an opportunistic side payment. It is a competing salary structure.

What has emerged in this landscape are "specialists," facilitator organizations that provide turnkey service for DTOs, bridging the gap between criminal networks and the port personnel whose access they require. Without them, moving volume through maritime shipping would be a far more difficult proposition.

How Recruitment Works

Three vectors. Each surfaces differently. Each is exploited differently. Standard HR processes catch none of them.

Financial Pressure. Dock workers earn modest wages in close proximity to high-value criminal logistics. The 'Ndrangheta investigation referenced above documented commission rates of 7 to 20 percent of cargo value per facilitated shipment.[3] Skuld's industry guidance on Latin American narcotics smuggling describes the same recruitment dynamic across Colombia, Ecuador, Peru, Mexico, Brazil, and Venezuela: traffickers "require access to the port areas usually through the recruitment of corrupt drivers, transport companies, stevedores, and container yard workers" in order to load drugs into containers.[4]

Social And Community Ties. Port employment in many LATAM terminals concentrates on workers from the same neighborhoods, the same families, and the same migration corridors. Criminal organizations with local roots do not approach strangers. The initial conversation arrives through a known acquaintance or a member of the worker's extended family who has already crossed the line. By the time a recruitment ask is articulated, a relationship of obligation already exists. This is the vector that makes insider recruitment invisible to standard HR processes.

Coercion. In environments where criminal organizations exercise effective control over port-adjacent communities (documented in Guayaquil, in zones surrounding Santos, and in specific corridors in Colombia and Mexico),[5] refusal is not a safe option. Workers comply not from incentive but from the absence of an alternative. Violence against workers who resist

is documented. A single example, communicated through the same family and neighborhood networks described above, is sufficient to establish the rule.

A common scenario at LATAM ports today: key personnel receive WhatsApp messages containing specific physical threats against them and their families, often with photos or videos of their homes or loved ones paired with a monetary offer to look the other way or provide information. The message itself is the coercion mechanism.

What Insiders Actually Provide

Different roles solve different bottlenecks. Each tier represents a distinct detection challenge.

Insider involvement is not an isolated category; it maps to the operational role of the recruited worker. The value provided to the criminal network varies sharply by access tier.

Manifest and container positioning. Container codes, bay assignments, and movement timing. The 2018 "PIN-code fraud" technique first detected in Rotterdam, in which criminal networks misappropriate the unique container reference code needed to collect cargo, illustrates how a single piece of insider-provided data can compromise an entire shipment.[2] Without it, no other tier of insider access matters, because the criminal network does not know which container to act on. This is the foundational layer.

Inspection routing. Which containers are flagged for scanning, when, and by whom. This information sits with customs supervisors and port security staff. Insider access at this tier converts a probabilistic problem (will my container be scanned?) into a deterministic one (I know it will not be).

Physical yard access. The rip-on/rip-off operation: locate the container, break the seal, load or unload the product, replace the seal with a high-fidelity replica. This requires dock labor or yard supervisors with legitimate physical access during the relevant window. The act itself takes minutes; the access required to perform it without observation takes coordination across multiple roles.

Digital record access. The most valuable and least discussed tier: workers who can modify access logs, manifest entries, container movement records, or inspection outcomes after

the fact. As port operations digitize, this tier grows in value. A clean digital record is more durable than a clean physical operation, because it survives the retrospective investigation.

These tiers are not just four different jobs. They are four different access surfaces, each governed by a different system of record, each owned operationally by a different team. The criminal network treats them as a single coordinated capability. The terminal treats them as four unrelated operational domains. That asymmetry is the opening.

Why Standard Controls Don't Catch It

Port security was built for hostile actors trying to get in.

The structural argument is straightforward. Background checks, perimeter controls, scanner allocation, credentialed access: every layer of port security architecture assumes an actor who does not belong, attempting to move material that is not theirs. The insider threat reverses each of those assumptions. The actor belongs there. The credentials are valid. The movement is authorized. The material being moved is, on paper, somebody else's legitimate cargo. The architecture, by design, does not register what is happening, because nothing about it looks like an attack.

This inversion has four operational consequences:

The screening model is one-shot, the threat is continuous. Background checks run once, at hire, and capture history up to that moment. A worker hired clean in 2019 and recruited in 2022 generates no flag, because there is no mechanism that re-asks the question after onboarding. The European Commission's March 2026 EU Ports Strategy explicitly proposes an EU-wide framework for ongoing port worker background checks, with implementation targeted for 2027, precisely because no such framework currently exists.[6] Checks are also typically limited to local government records, rather than searched against international databases or cross-referenced with social signals that would surface criminal associations, financial distress, or community ties to known networks.

The unit of analysis is the individual, the unit of compromise is the role. Existing controls are designed to ask *"is this person trustworthy?"* The operationally relevant question is different: "is this combination of access, this week, consistent with how this role normally functions?" A specific worker may be unremarkable. The role being performed in an unremarkable way is the entire problem, because the role is what the criminal network actually rented.

Each event is authorized; only the sequence is anomalous. After-hours yard access on Tuesday, an unusual manifest query on Wednesday, an inspection hold released without scanning on Thursday. Each event, in isolation, is legitimate work performed by an authorized person. There is no individual anomaly to escalate. The signal is the sequence, and a security architecture organized around per-event authorization has no native concept of a sequence as a unit of review.

Detection is retrospective by design. By the time a seizure investigation in Rotterdam or Antwerp reverse-engineers the chain back to the departure port, the operation has typically run multiple times. The signals were present in the data the entire time. "Retrospective" is the operative word: it describes a security posture organized around explaining what happened, not interrupting what is happening. That is a defensible posture against an external threat where intrusions are discrete events. It collapses against an insider threat where the operation is continuous and the next shipment is already in motion.

Once security analyst at one LATAM port began looking at time and attendance records a pattern emerged where the arrival of a specific ship correlated with a 30% reduction in port personnel. Not once but every time a specific ship was in port. Upon interviewing employees the analyst learned that it was widely known amongst port personnel when bad actors planned to contaminate containers. Those attempts coincided with a specific ship with a Mediterranean route. Honest workers opted for sick leave or personal days instead of becoming witnesses to the illegal activity and becoming possible targets of the DTOs.

The Scale Problem

Detecting one insider is hard. Detecting a network of insiders is a different problem entirely.

Insider recruitment is sometimes discussed as a single-bad-actor story. The data does not support that framing. The volumes of cocaine now moving through LATAM ports require coordinated logistics across multiple container movements per shipment, and each movement requires its own insider facilitation. As Ecuador's 2024 seizures hit record levels, Belgian customs at the port of Antwerp recorded a sharp drop, from 121 metric tons seized in 2023 to 44 metric tons in 2024.[7] Enforcement pressure at one node redirects volume rather

than reducing it. Moving these amounts is not the work of one corrupted worker; it is the work of an embedded network.

Europol's investigations at Antwerp, Hamburg/Bremerhaven, and Rotterdam have documented this directly: insider corruption operates as organized internal networks, distributed across logistics companies, customs services, and security operations simultaneously.[2] Workers in different departments, on different shifts, with different access levels, coordinate to facilitate a single shipment. The structure is deliberate. It is designed to defeat exactly the kind of single-actor monitoring that most port security operations have in place.

This changes the detection problem fundamentally. Identifying a single corrupted worker through behavioral monitoring is difficult but tractable; enough anomalies eventually accumulate to draw attention. Identifying the pattern that connects multiple corrupted workers across different roles, departments, and shifts is a different capability entirely. It requires entity-level intelligence: the ability to ask not just "*did this worker behave anomalously?*" but "*do these workers, individually unremarkable, share an unusual pattern of co-occurrence with the same flagged containers, the same vendors, or the same incidents?*" That question cannot be answered by any system most LATAM terminals operate today, because the question itself is not in the operational vocabulary of those systems.

The insider threat is not a personnel problem. It is a behavioral intelligence problem at the level of the network, not the worker. That is a category of question most port security operations are not yet asking.

What Detection Actually Requires

The hard part is not collecting more data. The hard part is asking the data a question it has never been asked before.

It is tempting to describe the gap as a data integration problem and stop there. That framing is incomplete and, in practice, misleading. Most LATAM terminals do not lack data. They lack the operational question that would make their existing data answer something useful. Insider activity is, by construction, indistinguishable from legitimate work at the level of any single event. It only becomes visible when the data is interrogated by a question shaped to the actual threat model: not "what happened?" but "which combinations of people, access,

and cargo have co-occurred in ways the legitimate operating tempo of this terminal does not explain?"

Four shifts are required, in this order. The order matters. Reversing them is what produces the dashboards that nobody uses.

From event to entity. Most port systems are organized around events: a swipe, a query, a manifest change, an incident report. Insider operations are organized around entities: this worker, this vendor, this vessel, this container, this corridor. An event-organized system can describe a shift; only an entity-organized system can describe a relationship. The first capability to build is not a dashboard. It is an entity model in which every event, across every source system, attaches cleanly to the people and things it actually concerns.

From anomaly to co-occurrence. No single event in an insider operation is anomalous, which is why per-event detection produces noise and misses the pattern. The relevant signal is co-occurrence: the same three workers, on the same shift, around the same vendor, in proximity to the same flagged containers, across three different facilitated shipments. No individual anomaly. The co-occurrence is the anomaly.

From incident to dossier. A single incident almost never proves insider involvement. A worker associated with three flagged containers across eighteen months does. But "associated with" is not a field in any operational system; it is the product of documentation that accumulates against an entity over time. Without a dossier layer, every investigation starts from zero. The entity has no memory. Insider networks rely on that.

From internal data to external signals. Recruitment pressures (financial distress, criminal associations, community ties) surface in external sources, not in terminal systems. A detection architecture limited to data the terminal itself generates is, by construction, blind to the recruitment vectors in Section 2. The terminal sees the access. The recruitment lives somewhere else.

A final note on what this is not. It is not a recommendation to buy more cameras, scanners, or readers. Most LATAM ports already have these. It is also not a call to consolidate every system into one. What is required is a thin entity-and-co-occurrence layer that reads across existing systems without replacing them.

Sources

1. UN News, UN-Backed Programme Logs Record High Cocaine Seizures at Seaports in Latin America and the Caribbean (2018), citing UNODC Container Control Programme: more than 720 million containers move by sea annually, transporting roughly 90 percent of global cargo.
2. Europol and the Security Steering Committee of the Ports of Antwerp, Hamburg/Bremerhaven, and Rotterdam, Criminal Networks in EU Ports: Risks and Challenges for Law Enforcement: Focus on the Misappropriation of Container Reference Codes (The Hague: Europol, 30 March 2023). Designation of port personnel corruption as the "key enabler" of criminal infiltration; PIN-code misappropriation technique first detected at Rotterdam in 2018.
3. Europol news release, Italian Operation Takes Down Corrupt Port Workers Facilitating 'Ndrangheta Drug Trafficking Activities: Customs Officer Features Among the Arrested (6 October 2022). Joint Italian Guardia di Finanza, Europol, and Eurojust operation at Gioia Tauro: 7–20 percent commission to corrupt dock workers; 3 percent to corrupt customs officer for altered x-ray scan; over 4 metric tons of cocaine seized; estimated street value above €800 million.
4. Skuld P&I, Colombia: Drug Smuggling: Update (2022). Recruitment of corrupt drivers, transport companies, stevedores, and container yard workers as the operational mechanism behind container contamination across Latin American departure ports.
5. International Crisis Group, Curbing Violence in Latin America's Drug Trafficking Hotspots, Report No. 108 (March 2025). Documentation of organized-crime control of port-adjacent communities in Guayaquil, Santos, and corridors in Colombia and Mexico.
6. European Commission, EU Ports Strategy: Securing Competitive, Resilient and Sustainable European Ports (March 2026). Proposes EU framework for port worker background checks (targeted 2027) and frameworks for third-country port assessments, building on the European Ports Alliance.
7. InSight Crime, InSight Crime's 2024 Cocaine Seizure Round-Up (April 2025). Belgian customs seized 44 metric tons of cocaine at Antwerp in 2024, down sharply from 121 metric tons in 2023; analysis attributes the shift in part to enforcement-driven displacement.

About the Ports Under Pressure Series

This is the second paper in a four-part series examining the evolving challenges facing Latin American container ports. Paper One examined how criminal networks select ports as departure nodes. This paper, Paper Two, examines the insider threat that makes those ports operationally viable. Paper Three will address the fragmentation of port security systems and what that fragmentation costs. Paper Four will define the integrated intelligence architecture required to close the gap. To receive remaining papers in the series or to discuss how these issues are affecting your port or terminal, contact us at tapestriisupport@aperia.com.

About Aperia

Aperia delivers ICM by Tapestrii, an intelligent case management platform that helps terminal operators and port authorities connect fragmented incidents, entities, and operational data to detect emerging risks earlier and strengthen decision-making in complex, high-stakes environments. We welcome dialogue with port operators, terminal managers, and security leaders committed to staying ahead of these dynamics. Learn more at www.aperia.com.

James Kuykendall is a former DEA Assistant Regional Director with extensive Latin America operations experience and a practicing maritime security consultant.

Viviana Lewis is a Product Manager at Aperia, leading product and global client success for ICM by Tapestrii.