TRANSPORTED ASSET PROTECTION ASSOCIATION

E-MAGAZINE • ISSUE 9 - 2026

VIGILANT



ASSISTED INTELLIGENCE

TAPATRON AI Assistant launch lifts value of data & intelligence for cargo security and supply chain resilience to its highest-ever level



The new FSR 2026 & TSR 2026 supply chain security Standards are now 'live' in EMEA

YOUR SUPPLY CHAIN SECURITY STANDARDS

On 15 September, the new 2026 revisions of TAPA's Facility Security Requirements (FSR) and Trucking Security Requirements (TSR) went 'live' in Europe, the Middle East & Africa (EMEA), replacing the 2023 versions of FSR and TSR.

In keeping with the Association's Standards' review and revision cycle, FSR and TSR are updated every three years, supported by feedback from our member companies using the Standards as a core part of their everyday supply chain security protocols.

The review process gives us an opportunity to make the implementation and use of FSR and TSR more efficient. Of course, our priority is to always protect the security intentions of both Standards, but we are always open to ways to make this process easier and more seamless. And, of course, every 3 years we take the important opportunity to ensure our security requirements are able to defend against new and emerging supply chain security risks.

Through this latest review, we believe FSR 2026 and TSR 2026 will bring greater security benefits and more efficiency to the TAPA Standards' certification process.

So, now, it is over to our members – with our continued support – to embrace the new Standards' revisions and to use FSR and TSR to help protect their supply chain operations.

Our Standards can be downloaded from the TAPA EMEA website, and our updated training courses are also available to book now.

In the coming weeks and months, we will once again start to roll out a series of translations of FSR and TSR as well as local language trainings to make the Standards as accessible as possible to our member companies.

I wish to personally thank everyone involved in the Standards' revision process, including our TAPA colleagues in the Americas and Asia Pacific, our Standards & Training Team in EMEA, and our Working Groups, who have all brought their valuable day-to-day knowledge and experience of FSR and TSR to the forefront of our evaluation, and worked tirelessly to deliver FSR 2026 and TSR 2026 for the benefit of the global TAPA Family.

The signs are good. FSR certifications have risen 13% in the last year and now cover facilities in 68 countries. TSR now spans trucking operations in 31 countries, up 15% YoY, and protects nearly 50,000 vehicles. As Thorsten Neumann always says, we are confident more will come.



TAPA EMEA

MARKUS PRINZ
Director, Standards & Training
TAPA EMEA

CONTENTS

PAGE 3
>100 delegates already registered for TAPA EMEA's *Spain Regional Conference* in Madrid – registration closing soon

PAGES 4-5
TAPA EMEA's President & CEO discusses the European Commission, AI, meeting in Madrid, our *2027 Annual Conference*, podcasting, and becoming a *2027 Premier Partner*

PAGES 6-9
Insider risk: the threat that never has to break in...

PAGES 10-11
Save the date for TAPA EMEA's *2027 Annual Conference* in Germany

PAGES 12-19
Turning a mountain of freight crime data into more resilient supply chains

PAGES 20-22
TAPA EMEA *2026 Premier Partner*, Securitas – Turning TAPA standards into a living security system

PAGES 24-31
>€90 million of losses from freight crimes occurring in August 2026, as major losses average €3.5m

PAGES 32-34
TAPA EMEA *2026 Premier Partner*, Sensos – Stop chipping away at the gap. Close it.

PAGE 35
Are you tuning in to our *TAPA TALKS* podcast?

PAGES 36-37
Are you ready to become a TAPA EMEA *2027 Premier Partner*?

PAGES 38-43
South Africa's freight crime challenge

PAGES 44-45
Another 68 TAPA FSR, TSR & PSR certifications in 22 countries

>100 DELEGATES ALREADY CONFIRMED FOR TAPA EMEA'S REGIONAL CONFERENCE IN SPAIN – REGISTRATION CLOSING SOON...

Already over 100 cargo security and supply chain resilience professionals in Spain have registered as delegates for TAPA EMEA's Regional Conference in Madrid on 21 October 2026.

If protecting supply chain operations in Spain is important to your business, and you want to hear updates on freight crime trends and loss prevention from Spain's leading law enforcement agencies, you should register too – but please note, **registration is closing soon.**

The event will open with a presentation from General Cortés of Guardia Civil before Filipe de Almeida, TAPA EMEA's Regional Ambassador for Spain, explains how the Association's intelligence database and supply chain security standards are helping manufacturers and logistics providers protect their operations against criminal attacks. The audience will also hear a TAPA EMEA members' perspective from Natalia Merino Macedo of Amazon.

In keeping with the security certification theme, Carles Cardona Masfarré of Auditoria will help delegates understand how TAPA EMEA Standards' audits help companies detect vulnerabilities in their security protocols – because criminals do this for them.



Participants will also hear from Begoña de Madrid and Carmen Jordá Sanz from the Professional Association of Criminologists of the Community of Madrid (CPCM) with their insight into crime in the transport and logistics sector.

The event will conclude with two Q&A Panels. Panel 1 will focus on secure parking and the need to reinforce the necessary trucking stops en route. Panel 2 will give the law enforcement viewpoint with contributions from senior police representatives of Guardia Civil, the National Police Corps (CNP), and and Mossos d'Esquadra.

The Spain Regional Conference will conclude with a Networking Reception.

Please note: all presentations and panel discussions will be in Spanish.

We hope to welcome you in Madrid.

REGISTER NOW...



TOTALLY TAPARIZED



TAPA EMEA's President & CEO, Thorsten Neumann, shares his personal updates and views on the latest activities aimed at delivering more benefits to the Association's biggest-ever membership network and takes a look at other news and events impacting cargo security and supply chain resilience across our region...

TALKING WITH THE EUROPEAN COMMISSION...

I am not the only member of our team doing a lot of travelling to industry events in recent weeks.

We were also delighted to be invited to participate in *Connecting Europe Days*, Europe's mobility flagship event, and TAPA EMEA's Markus Prinz and Pana Laimos were in the audience in Brussels to hear Ursula von der Leyen, President of the European Commission, give the opening address at this special 3-day exchange.

Markus and Pana joined 4,500 participants taking part, including politicians, financial institutions, industry representatives, transport stakeholders and the European Commission to discuss concrete measures and exchange good practices on creating a competitive, resilient, safe and sustainable transport sector in Europe, and to ensure the strategic resilience of essential supply chains. This included discussions on the future of infrastructure funding and financing.

We also had the opportunity to share our thoughts and experiences on secure truck parking as Markus joined a special roundtable discussion on *'Safe truck parking as the backbone of resilient and green road freight corridors.'* **We will continue our close collaboration with the European Commission on this important topic.**



OUR AI INTELLIGENCE JOURNEY IS UNDER WAY

I am loving our new TAPATRON AI Assistant!

If you were one of the >300 TAPA EMEA members who joined our latest TIS *'Deep Dive'* webinar this month, you will have seen our new AI tool in action. And, in this issue, our TIS Manager, Satya Roy, explains more about TAPATRON AI Assistant, and how the powerful intelligence it can interrogate will help you make faster and smarter decisions to make your supply chains more secure against ever-increasing freight crime risks.

We will continue to learn about AI capabilities and what more we can do. **The TAPATRON AI Assistant is an amazing start on that journey. Check it out...**



THE BIG DATE IN 2027

I hope your 2027 calendars now have a very important date saved – 9 & 10 June 2027 - because that's when we will be returning to Metronom Theater Oberhausen for our next TAPA EMEA *Annual Conference*.

We have announced the date and venue now for three very important reasons to support our members: (1) to ensure you save the date, (2) to allow you to book your hotels while there is plenty of choice available and to get the best accommodation rates, and (3) for those delegates needing to book flights to join us, the chance to find the most cost efficient option. We will issue a further communication when we open our registration process.

This is the one event in 2027 you won't want to miss. See you there!



MAKING IT TO MADRID

Time is running out to register for our next TAPA EMEA *Regional Conference* in Madrid on 21 October 2026.

If you want to understand more about freight crime risks facing supply chain operations in Spain, you should be there...

As you will have seen on page 3 of this issue, we have brought together a host of leading speakers from Spain's law enforcement agencies and industry to address a problem, which based only on incidents reported to our TAPA Intelligence System (TIS), caused over €386 million of losses for supply chains in Spain in just 18 months or 547 days – and this value is only based on 13% of cargo crime reports to TAPA EMEA telling us their loss value. This event might help stop your business from becoming a future victim.

REGISTER NOW...



BECOMING A 2027 PREMIER PARTNER...

Our annual *Premier Partner* programme is now well-established and gives leading providers of supply chain security products and services a range of opportunities to showcase their solutions to the TAPA EMEA Family using a unique, 12-month package of benefits.

As you will see in this issue of ***Vigilant***, we have now launched our *2027 Premier Partner* programme with even more benefits. As always, we offer our current *Premier Partners* the first option to renew their partnerships with us for the coming year, before we reach out to other companies which have expressed an interest in joining the programme.

These opportunities will be offered in the order companies have approached us. As we only have a limited number of *Premier Partner* packages available for 2027, if you want to learn more about the available benefits, please contact me at **Thorsten.Neumann@tapaemea.org**

TAPA EMEA PREMIER PARTNER 2027

TALKING TAPA IN PODCAST 4

Episode 4 of our *TAPA TALKS* podcast is out at the beginning of October and will be available to download from Spotify, Amazon Music, Apple, and YouTube.

PODCAST

This time around, we take a deeper look inside TAPA EMEA to explain about the support system infrastructure we have built, the instant visibility we now have across our membership network, and why this is so important to help us manage our growth in a fair and equitable way for our entire member community. It's an opportunity to understand the reasons behind our decisions and to appreciate the benefits this approach enables us to deliver.

Listen in... and I welcome your feedback.

TAPA EMEA'S FAMILY IS GROWING... *welcome*

Introducing the latest companies to join us in our Europe, Middle East & Africa region...

9 COMPANIES & ORGANISATIONS

6 COUNTRIES

COMPANY	MEMBERSHIP TYPE	COUNTRY	WEBSITE
Anika Trans Sp. Z o.o.	Country Full	Poland	VISIT WEBSITE >
ASICS Europe B.V.	Full	Netherlands	VISIT WEBSITE >
Delivar AG	Full	Switzerland	VISIT WEBSITE >
Haleon Trading Services Limited	Full	United Kingdom	VISIT WEBSITE >
Nicholas Gilbert El - Agilsur Conseil	Consultancy	France	VISIT WEBSITE >
Telemetry Systems Limited	Country Security Service Provider	United Kingdom	VISIT WEBSITE >
Transwhite-Transportes,Unipessoal Lda	Country Full	Portugal	VISIT WEBSITE >
VARS Technology Ltd	Country Security Service Provider	United Kingdom	VISIT WEBSITE >
We Love Transport B.V.	Country Full	Netherlands	VISIT WEBSITE >

TO SEE ALL OUR 2026 MEMBERSHIP CATEGORIES, BENEFITS & COSTS CLICK HERE >

THE THREAT THAT NEVER HAS TO BREAK IN

Insider risk is the supply chain's quietest crisis – and the one we are least organised to face

By Filipe Joel de Almeida – Regional Ambassador for Portugal, Spain & Africa, TAPA EMEA

We have become very good at the perimeter. Fences, bollards, seals, geofencing, camera analytics, a control tower watching a map of moving dots across Europe. And yet, incident after incident, the post-event review arrives at the same uncomfortable place: nobody broke in. Someone already had the key, the code, the password — or simply knew the answer to a question they should never have been asked.

That is the insider problem in a sentence. It does not defeat our controls; it is issued them on day one.

I want to argue three things in this article. First, that the supply chain is structurally more exposed to insider risk than almost any other sector, for reasons that have nothing to do with the quality of our people. Second, that what the modern insider sells has changed, and that this makes insider risk the definitive test of security convergence. And third — because this is what our members actually need — that there is a practical programme of work available to us, most of which costs governance rather than capital.

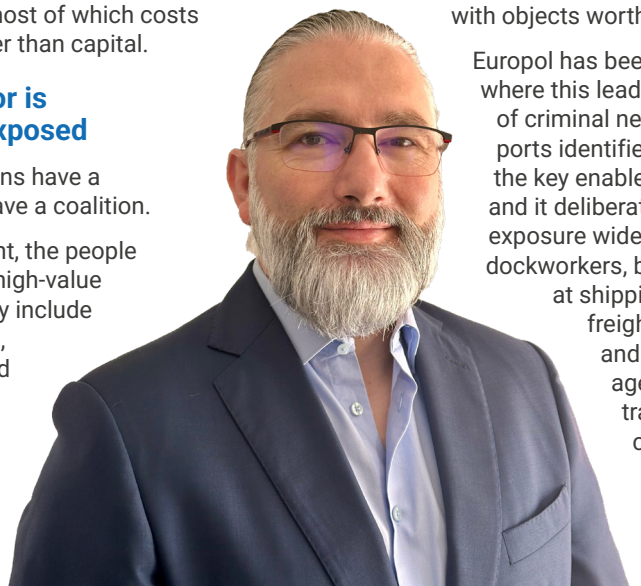
Why our sector is structurally exposed

Most organisations have a workforce. We have a coalition.

On any given night, the people with hands on a high-value consignment may include direct employees, agency staff hired that week, a self-employed driver subcontracted by a haulier we contracted, terminal handlers, a customs broker, a cleaning crew, a refrigeration engineer and an IT integrator with remote access to the warehouse management system. Our perimeter is not physical. It is contractual — and trust is transitive in a way that our due diligence almost never is. We assure the first link. We rarely audit the third.

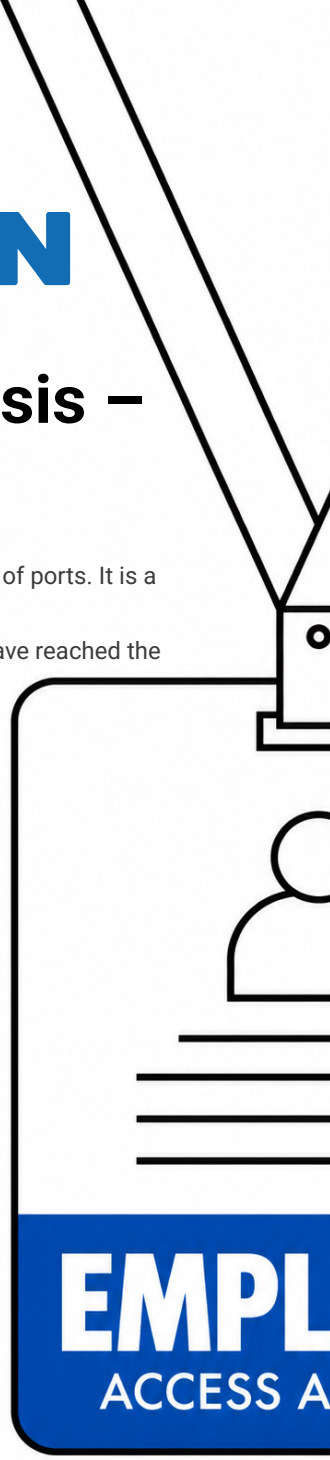
> *'Supply chain is structurally more exposed to insider risk than almost any other sector, for reasons that have nothing to do with the quality of our people.'*

Layer onto that the conditions of the work itself: high turnover, seasonal peaks staffed at speed, night shifts, lone working, thin margins, and a large population of people who are paid modestly to be alone with objects worth a great deal.



Europol has been consistent on where this leads. Its analysis of criminal networks in EU ports identified corruption as the key enabler of infiltration, and it deliberately drew the exposure wide — not only dockworkers, but personnel at shipping lines, freight forwarders and shipping agents, importers, transport companies and terminals. That list is not a description of ports. It is a description of us.

European legislators have reached the same conclusion. The *Critical Entities Resilience Directive (EU) 2022/2557* requires critical entities to manage employee security, and explicitly obliges Member States to ensure that the personnel of external service providers are taken into account when defining who exercises critical functions. Recital 32 goes further still, naming the misuse of access rights by employees and contractors as a concern of growing importance. The law now assumes an extended trusted population. Most of our HR systems do not.



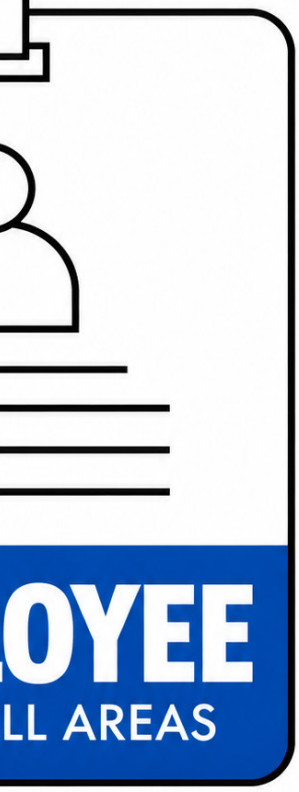
What the insider actually sells

The traditional image of the insider is the driver who leaves a trailer unlocked, or the picker who walks out with a box. That still happens. But the economics have moved, and they have moved decisively towards information.

The most valuable thing an insider can offer today is not the goods. It is the answer to a question: what is on the vehicle, when does it leave, which route, where does it stop for the night, which seal, which yard, which alarm code, which container reference.



A single person with a query screen and a mobile phone is now worth more to a criminal network than a team of thieves — and carries a fraction of the risk.



Europol's work on EU ports documented exactly this shift, describing the misappropriation of container reference codes — PIN-code fraud — as a growing method for extracting containers by impersonating the legitimate consignee. That is a data compromise executed with a lorry. It sits in no one's silo.

This is why I have come to see insider risk as the definitive convergence problem. A recruited insider does not respect our organisation chart. The act combines physical access, system access and fraud, and if those three capabilities report to three different directors, use three different toolsets and hold three different incident logs, then the insider lives comfortably in the seams between them. Nobody owns the whole picture, so nobody sees the whole picture.

The numbers reinforce how European this problem is. Verizon's 2025 *Data Breach Investigations Report* found that around 29% of breaches in EMEA originated inside the organisation — against 5% in North America and 1% in APAC — with a substantial share attributable to unintentional error rather than malice. The Ponemon Institute's 2026 *Cost of Insider Risks* study, sponsored by DTEX, put the average annual cost of insider risk at approximately US$19.5 million per organisation, up from US$17.4 million the previous year.

> ***'On any given night, the people with hands on a high-value consignment may include direct employees, agency staff hired that week, a self-employed driver subcontracted by a haulier we contracted, terminal handlers, a customs broker, a cleaning crew, a refrigeration engineer and an IT integrator with remote access to the warehouse management system.'***

Set that alongside our own intelligence. TAPA EMEA's systems recorded more than 157,000 cargo crimes across 129 countries in 2022–2024; fewer than 6% of those reports carried a loss value, and those alone totalled some **€2.7 billion.** We are not short of evidence that our supply chains are being attacked. We are short of evidence about how often the attacker was already inside — because we very rarely record it that way.

Recruitment is a process, not a decision

We tend to imagine the malicious insider as a moment of moral failure. In practice it is usually a slope.

Ponemon's 2026 study attributes roughly 53% of insider incidents to negligence, 27% to malicious insiders and 20% to credential theft. Read that carefully: in about three quarters of cases, the insider is not a traitor. They are careless, or they have been outplayed. That should reshape where we spend our energy.

For the recruited insider, the pattern is depressingly consistent. It begins with identification — a social media post, a driver forum, a relative, an approach in a lorry park. Then comes the small favour: a photograph of a manifest, confirmation of a departure time, the name of the site handling a particular customer. It is trivial, it is deniable, and it is paid. Only afterwards does the leverage arrive, because once the first favour exists, refusing the second has a price.

Criminal recruitment is now an industrialised function. Europol's June 2026 assessment mapped 731 criminal

> ***'The most valuable thing an insider can offer today is not the goods. It is the answer to a question: what is on the vehicle, when does it leave, which route, where does it stop for the night, which seal, which yard, which alarm code, which container reference.'***

CONTINUED ON PAGE 8 >



networks operating in the EU with more than 400,000 members, and law enforcement across Europe has repeatedly warned that encrypted messaging and social platforms are used to source recruits at scale, often targeting the young and the financially pressured. The EU's December 2025 action plan against drug trafficking explicitly commits to countering the recruitment of port workers and the use of insiders.

And coercion belongs in this picture too. Where staff and their families live close to the operation, the threat is not always financial.

Why we do not detect them

Because detection is a correlation problem, and we have built our organisations to prevent correlation.

No single indicator means anything. A driver who takes an unusual route once avoided a traffic jam. A warehouse supervisor querying high-value stock outside their area was covering for a colleague on leave. A resignation is a resignation. The signal only exists at the intersection — access control logs, system query logs, rota and lone-working data, loss history, and HR events such as grievances, disciplinary actions or



a sudden change in circumstances. Almost no logistics business brings those together.

Nor, in Europe, can we simply merge them and see what happens. Data protection law, works councils and employment law constrain what we may monitor, on what basis, for how long. I would argue this is not an obstacle but a design specification. An insider risk capability that cannot survive contact with a data protection impact assessment is not a capability; it is a liability waiting for a regulator.

Time is the other reason we fail. Ponemon reports an average containment time of 67 days, with only about 13% of incidents contained inside 30 days — and a sharp cost penalty for cases that run beyond 90. Insider cases are slow because they are ambiguous, because the evidence is entangled with employment rights, and because nobody wants to be wrong about a colleague.

Finally, there is a quieter failure: classification. Insider events are routinely closed as “HR matters” or absorbed into unexplained shrinkage, and never enter the security data set at all. What we do not count, we cannot manage — and we certainly cannot fund.

> *‘Data protection law, works councils and employment law constrain what we may monitor, on what basis, for how long. I would argue this is not an obstacle but a design specification.’*

Ten things you can do

1. **Name it and own it.** Write a definition, get a policy approved at board level, and appoint one accountable owner. Then set up a standing working group — Security, HR, IT, Legal or the DPO, Procurement and Operations — with a charter, a quorum and a meeting rhythm. Insider risk fails most often because it belongs to everyone (and therefore to no one).
2. **Map the trusted population, not the payroll.** List every person who can touch the asset or the data about the asset, including agency staff, subcontractors and remote system integrators. Classify them by what they can reach, not by their job title or seniority.
3. **Screen proportionately, and flow it down contractually.** Match vetting depth to access, repeat it periodically rather than once at hire, and require the same of subcontractors in writing. The TAPA Standards’ familiar qualifier — as permitted by local law — is not a licence to skip screening; it is an instruction to find the lawful method in each jurisdiction.
4. **Compartmentalise the information.** Apply need-to-know to manifests as rigorously as we apply it to pallets. Mask value and product descriptors for roles that do not require them, and restrict how many people can see the complete picture of load, route and timing in one place.

5. **Enforce least privilege in both domains.** Give a badge the same discipline as a login. Joiners and leavers usually get attention; movers rarely do, and privilege accumulates quietly across a long internal career.
6. **Design out the lone decision.** No single individual should be able to release, reroute, re-label or authorise a high-value consignment alone. Dual authorisation and segregation of duties do more to deter recruitment than any camera, because they make the insider's offer worthless without an accomplice.
7. **Make reporting easy, safe and rehearsed.** The EU Whistleblower Directive gives the legal frame; trust delivers the results. Train people to recognise a grooming approach and to report being approached without fearing they will be treated as suspects. Very often, the first person who knows is the person being recruited.
8. **Correlate – lawfully.** Start deliberately small: three or four data sources, a defined and documented set of risk indicators, a completed impact assessment, agreed retention periods, and mandatory human review before any action is taken about any individual.
9. **Rehearse the response before you need it.** An insider case is a security investigation, an HR process, a legal matter and a customer conversation at the same time. Decide in advance who authorises, how evidence is preserved so that it remains admissible, when law enforcement is engaged and who speaks to the client. The first case should not be the rehearsal.
10. **Measure leading indicators.** Incident counts tell you about last year. Track vetting coverage across the extended workforce, access reviews completed on time, mean time to revoke access on exit, dual-authorisation exceptions, and the reporting rate through your speak-up channel – where a rise is usually good news, not bad.



> *'A single person with a query screen and a mobile phone is now worth more to a criminal network than a team of thieves — and carries a fraction of the risk.... The numbers reinforce how European this problem is. Verizon's 2025 Data Breach Investigations Report found that around 29% of breaches in EMEA originated inside the organisation.'*

The compliance tailwind is finally here

For years, insider risk lost the budget argument because it lacked a regulatory hook. That has changed. Member States were required to identify their critical entities under the CER Directive by 17 July 2026, and transport and logistics operators across the region are being designated now — bringing employee security management, defined critical roles, access rights and background check procedures into the scope of supervised obligations. NIS2 covers the digital half of the same person. The 2026 revisions of the TAPA Standards continue to require screening and vetting records as an auditable matter of fact.

Those of us who have struggled to fund this work now have three independent arguments to make. We should use them.

Trust is the control, not the vulnerability

The instinctive response to insider risk is surveillance. I would urge caution. An organisation that treats every employee as a suspect manufactures precisely the alienation that criminal recruiters look for. The insider programme that damages morale is not a neutral cost — it is a threat multiplier.

The inversion is more useful. The strongest insider control in any logistics operation is a workforce that is fairly treated, properly supervised, clear about what good looks like, and confident that saying someone approached me at the truck stop last night will be met with support rather than suspicion.

We cannot vet our way to zero. What we can do is make sure that no single person is ever left alone with a decision worth more than their annual salary — and that the person who is approached knows exactly who to tell.





TAPA EMEA

2027 ANNUAL CONFERENCE

Metronom Theater

9 & 10 June 2027

Oberhausen, Germany

SAVE THE DATE...

TAPA EMEA's *2027 Annual Conference* will welcome over 800 supply chain and security professionals from across the Europe, Middle East & Africa region for two unique days of learning, intelligence sharing and networking.

JOIN US - & LET'S GET CONNECTED...



A UNIQUE & DEDICATED VENUE FOR THE CARGO SECURITY & SUPPLY CHAIN RESILIENCE EVENT OF THE YEAR IN THE EUROPE, MIDDLE EAST & AFRICA REGION...
REGISTRATION NEWS TO COME...

BOOK YOUR HOTEL & TRAVEL NOW FOR THE BEST RATES...




EUROPOL & LEA
UPDATE & Q&A PANEL
SPEAKERS
JENS LIEDHEGENER
THORSTEN HEIMANN


WE'RE
BACK IN
2027
PA EMEA ANNUAL CONFERENCE - THE RETURN
SAVE THE DATE - 9 & 10 JUNE 2027
Protection Association
Transported Asset Protection Association
KASSE

TURNING A MOUNTAIN

OF FREIGHT CRIME DATA INTO MORE RESILIENT SUPPLY CHAINS

TAPATRON: Making TIS Intelligence Faster, Smarter and More Actionable

A special report by Satya Roy, TIS Manager, TAPA EMEA...

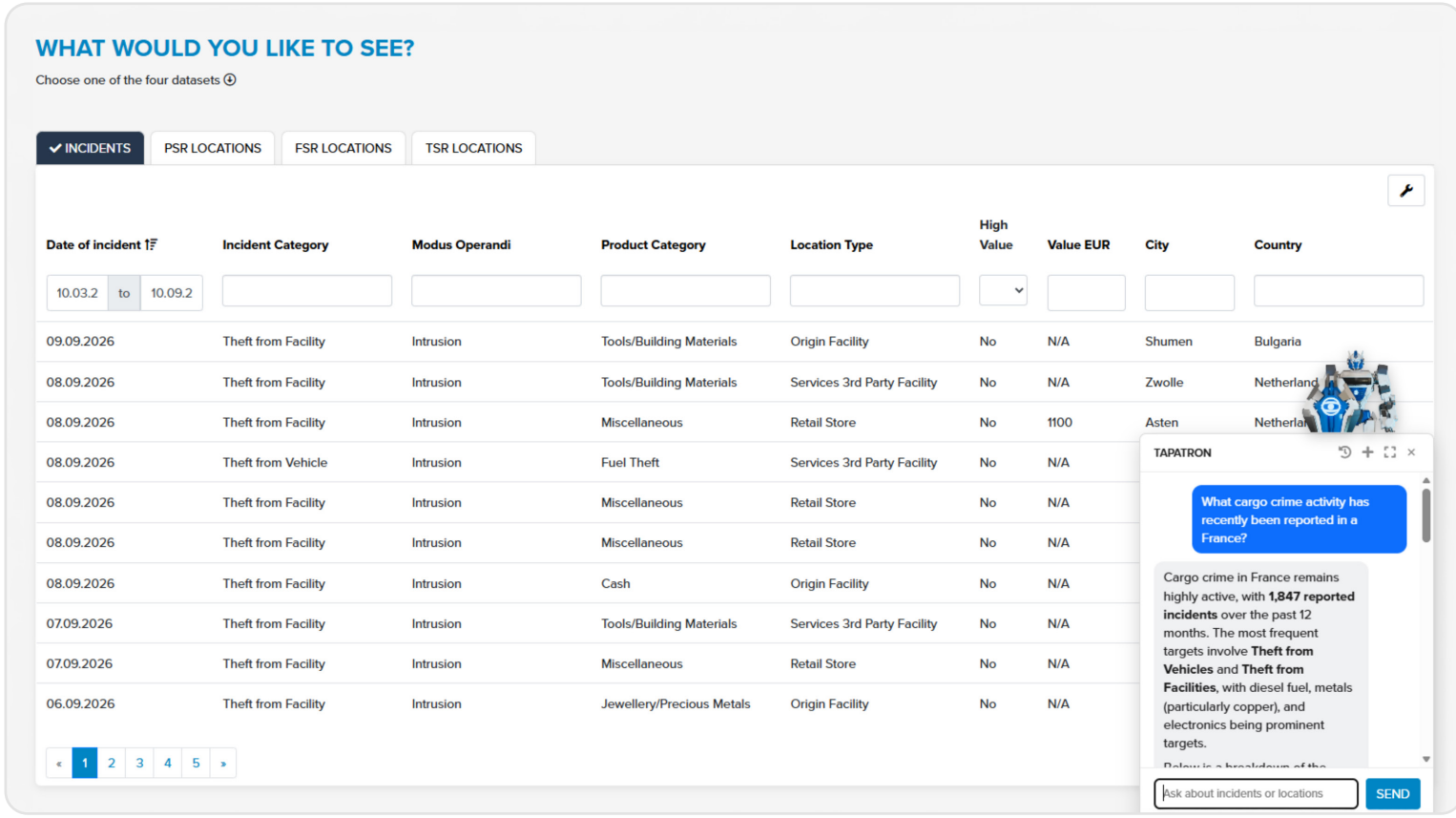
In cargo security, having access to intelligence is only the first step. The real challenge is being able to find the right information, understand its relevance and turn it into a practical security decision – quickly.

This is where the **TAPATRON AI Assistant** adds a new dimension to the TAPA Intelligence System (TIS). As the volume of cargo crime intelligence continues to grow, TAPATRON provides an AI-supported way for users to interact with TIS, making it easier to explore information and obtain relevant insights. Rather than replacing the knowledge and experience of security professionals, TAPATRON is designed to help them navigate intelligence more efficiently and spend more time assessing risks and deciding what action should be taken.





CONTINUED ON PAGE 14 >



From searching data to asking questions

One of the key benefits of TAPATRON is the ability to interact with TIS intelligence in a more natural and accessible way.

Traditionally, obtaining intelligence from a large database can require users to know exactly what they are looking for, select multiple filters, review individual incidents and then connect the information themselves. While these capabilities remain valuable, TAPATRON provides an additional layer of intelligence support by allowing users to explore TIS information through **natural-language interaction**.

This means that instead of thinking primarily in terms of database searches, users can approach TAPATRON with a question or intelligence requirement.

For example, a security professional may want to understand:

- What cargo crime activity has recently been reported in a particular country?
- What types of cargo are most frequently targeted in a specific area?
- What modus operandi are being used?
- Are there recurring patterns along a particular route?
- What should be considered when assessing a specific cargo security risk?

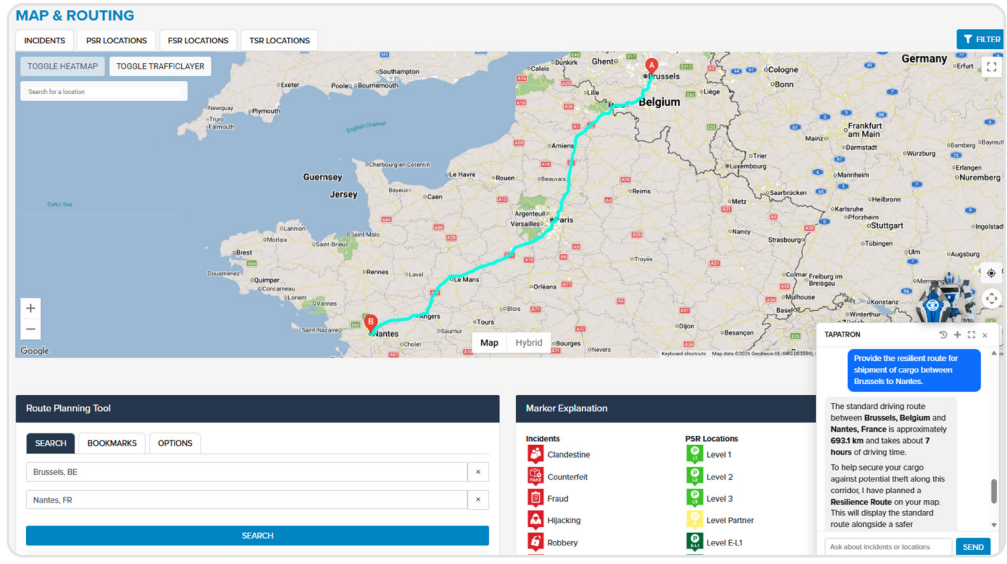
TAPATRON can help users navigate the available intelligence and bring relevant information together more efficiently.

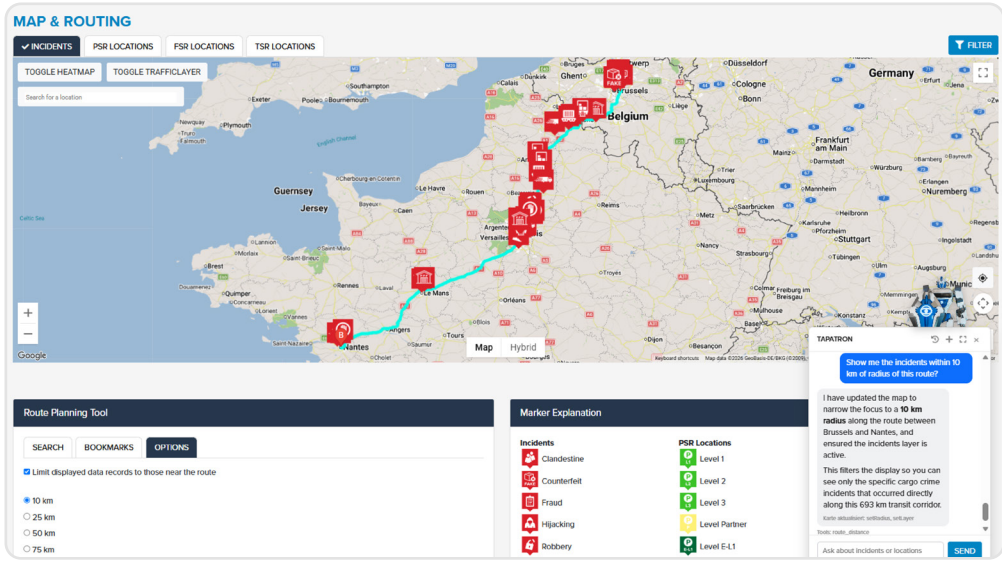
This makes the process of using TIS more intuitive, particularly when a user is trying to move from a broad security question towards a more focused intelligence assessment.

Faster access to relevant freight crime intelligence

Time is an important factor in cargo security.

Threats can change quickly, criminal methods can evolve, and new incidents can alter the risk picture. TAPATRON supports this requirement by reducing the effort involved in navigating large volumes of information.





Instead of manually working through numerous records before reaching a useful insight, users can use the AI Assistant as an intelligent starting point for their analysis. TAPATRON helps users locate and explore relevant information, allowing them to reach the intelligence they need more efficiently.

The value is therefore not simply speed for its own sake. Faster access means security professionals can devote more time to the activities that require human judgement—interpreting the threat, assessing exposure, and determining the appropriate response.

This is particularly useful when intelligence is required for time-sensitive activities such as…

- Route assessments
- Security reviews
- Incident investigations
- Management briefings

Turning questions into usable intelligence insights

The real advantage of TAPATRON becomes apparent when a user has a specific intelligence requirement but does not necessarily know which combination of filters or searches will provide the answer.

Consider a security manager preparing to evaluate a transportation route.

Rather than reviewing incidents individually, the user can use TAPATRON to help explore the relevant intelligence around the route, locations, and types of crimes involved. The resulting information can then support a wider assessment of potential exposure.

Similarly, when investigating an incident, TAPATRON can help users explore the broader context around the event. An individual cargo crime incident may provide information about a location, commodity, or criminal method, but looking at related intelligence can reveal whether the incident forms part of a wider pattern.

> ***'Faster access means security professionals can devote more time to the activities that require human judgement—interpreting the threat, assessing exposure, and determining the appropriate response.'***

This reflects one of the fundamental strengths of TIS: individual incidents become more valuable when they are considered collectively. The uploaded article notes that incidents can reveal patterns involving criminal behaviour, targeted commodities, locations, routes, and methods that may not be visible from a single event.

TAPATRON helps users navigate towards those wider insights more efficiently.

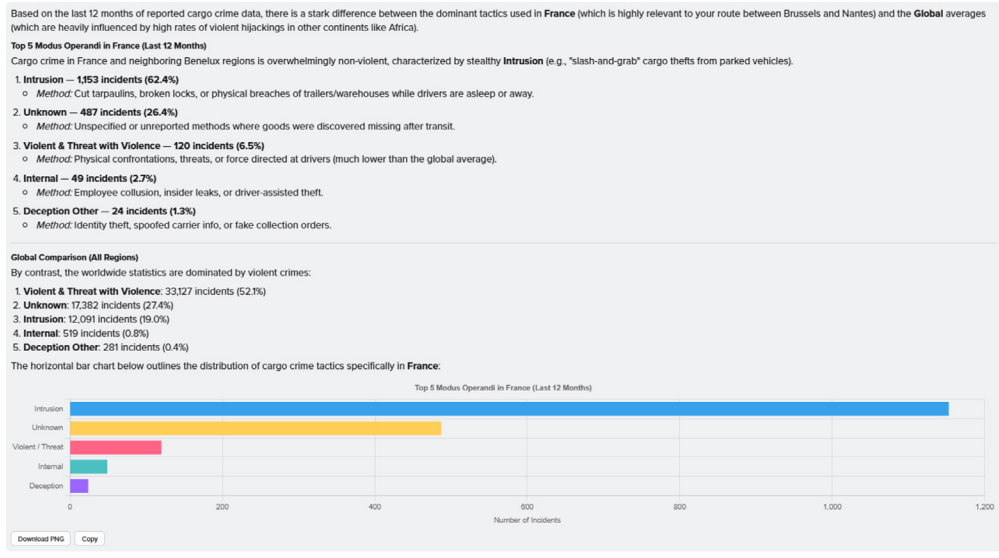
Helping users understand Modus Operandi in freight crimes

Understanding how criminals operate is an essential part of cargo crime prevention.

TIS already provides information on modus operandi, allowing users to identify common methods associated with cargo theft and other supply chain crimes. This intelligence can be used to review existing security controls and determine whether those controls remain appropriate for the threats being faced.

TAPATRON makes this intelligence easier to explore.

Users can use the AI Assistant to investigate questions around criminal methods and identify relevant intelligence within TIS. This can help transform historical incidents into useful preventive intelligence. The benefit is particularly important because criminal behaviour is not static. Criminals adapt their methods, target different commodities, and exploit vulnerabilities in transport routes, parking locations, warehouses and logistics facilities.



Based on the last 12 months of reported cargo crime data, there is a stark difference between the dominant tactics used in **France** (which is highly relevant to your route between Brussels and Nantes) and the **Global** averages (which are heavily influenced by high rates of violent hijackings in other continents like Africa).

Top 5 Modus Operandi in France (Last 12 Months)

Cargo crime in France and neighboring Benelux regions is overwhelmingly non-violent, characterized by stealthy **Intrusion** (e.g., "slash-and-grab" cargo thefts from parked vehicles).

1. **Intrusion — 1,153 incidents (62.4%)**
   - *Method:* Cut tarpaulins, broken locks, or physical breaches of trailers/warehouses while drivers are asleep or away.
2. **Unknown — 487 incidents (26.4%)**
   - *Method:* Unspecified or unreported methods where goods were discovered missing after transit.
3. **Violent & Threat with Violence — 120 incidents (6.5%)**
   - *Method:* Physical confrontations, threats, or force directed at drivers (much lower than the global average).
4. **Internal — 49 incidents (2.7%)**
   - *Method:* Employee collusion, insider leaks, or driver-assisted theft.
5. **Deception Other — 24 incidents (1.3%)**
   - *Method:* Identity theft, spoofed carrier info, or fake collection orders.

Global Comparison (All Regions)

By contrast, the worldwide statistics are dominated by violent crimes:

1. **Violent & Threat with Violence**: 33,127 incidents (52.1%)
2. **Unknown**: 17,382 incidents (27.4%)
3. **Intrusion**: 12,091 incidents (19.0%)
4. **Internal**: 519 incidents (0.8%)
5. **Deception Other**: 281 incidents (0.4%)

The horizontal bar chart below outlines the distribution of cargo crime tactics specifically in **France**:

CONTINUED ON PAGE 17 >

AEO GDP TAPA Transported Asset Protection Association QUALITY ISO 9001:2015 NSAI Certified ADR



WE'RE DRIVEN BY RESILIENCE

Operating 24/7, strategically planned secure transport routes to ensure critical goods are delivered efficiently and reliably to end users.

For more than 80 years, we have combined traditional values with innovation and technology to deliver efficient, cost-effective, and sustainable logistics solutions across the pharma, high-tech, e-commerce, airfreight, and food sectors.

Providing secure and compliant full trailer load transport services across Ireland, the UK, and Europe with a dedicated fleet of more than 200 driver-accompanied vehicles.

Tel: +353 (0) 1 835 5200 – 24/7 Operations & Monitoring Center. **Email:** cmaynard@caffreyinternational.com



TAPA EMEA's TIS Manager, Satya Roy, speaking at this year's *Annual Conference* in Oberhausen.

By helping users explore the available intelligence more efficiently, TAPATRON supports a more informed understanding of these changing threats.

Making TIS more accessible

An intelligence platform is most effective when its information can be used by the people who need it.

TAPATRON provides a more accessible way to engage with TIS intelligence. Its natural-language approach means that users can begin with the question they need to answer rather than necessarily having to understand the entire structure of the database first.

This can make TIS easier to approach for users with different levels of experience.

For experienced professionals, TAPATRON can act as a productivity tool that accelerates intelligence exploration. For newer users, it can provide a more intuitive entry point into the information available within TIS.

The result is a more connected interaction between the user and the intelligence platform.

From AI assistance to action

Ultimately, the value of TAPATRON is not the technology itself. Its value lies in what the technology enables TIS users to do.

Cargo crime intelligence only creates value when it contributes to better understanding and better decisions. TAPATRON helps shorten the journey from a question to relevant intelligence, allowing security professionals to move more efficiently through the stages of exploration, understanding, and assessment.

The final decision remains human.

A security professional must consider the operational environment, business requirements, existing controls, and the wider risk picture before deciding what action is appropriate. TAPATRON's role is to support that process by making relevant intelligence more accessible and easier to navigate.

> ***'TAPATRON provides a more accessible way to engage with TIS intelligence. Its natural-language approach means that users can begin with the question they need to answer rather than necessarily having to understand the entire structure of the database first.'***

This is why the introduction of TAPATRON represents the next important development of TIS. It brings an AI-supported interaction layer to a substantial cargo crime intelligence environment, helping users work with intelligence in a faster and more intuitive way.

Supporting better risk assessments

TAPATRON can also support the practical risk-assessment process.

Security professionals need to understand not only what happened, but also where the exposure exists and what it could mean for their operations.

For example, intelligence may indicate recurring cargo crime activity in a particular location or the use of a particular modus operandi. TAPATRON can help users explore the relevant information within TIS, which can then be used as an input into security assessments. The decision remains with the security professional.

This distinction is important. TAPATRON is not intended to replace professional experience or judgement. Its role is to make intelligence easier to access and search so that supply chain security specialists can concentrate on evaluating the information and deciding what action is appropriate. In practice, this creates a useful division of responsibility: TAPATRON helps find and organise the intelligence; the security professional interprets it and makes the decision.

With over 375,000 incidents across 166 countries contained within the TAPA Intelligence System (TIS) database, together with extensive information on certified facilities and trucking operators, and secure parking infrastructure, it provides members with a substantial resource for understanding and responding to supply chain risk.

TAPATRON AI now adds a new dimension.

By helping users simplify queries, apply filters, explore intelligence, and create professional dashboards, the AI Assistant is designed to make that resource more accessible and actionable…

- From searching to asking
- From data to insight
- From information to action

… And ultimately, from reacting to cargo crime to building smarter, more informed and more resilient supply chains.

TAPATRON: Turning TAPA EMEA intelligence into a conversation.

TIS CAPABILITIES

Powerful intelligence. Smarter decisions.

PLEASE TAKE ADVANTAGE OF THIS GREAT NEW BENEFIT...

'As we previewed at our *2026 Annual Conference* in Oberhausen, the first phase of our new TAPATRON AI Assistant is now 'live' and is the latest enhancement to our TAPA Intelligence System (TIS) as we continue to develop this fantastic intelligence tool. Our goal is to allow our members to more proactively use our freight crime data to improve their supply chain security.

'Using our TAPATRON AI functionality will help you quickly find and analyse information within our extensive cargo crime database, which now contains intelligence on over 375,000 freight theft incidents in more than 160 countries globally. I encourage you to familiarise yourself with this fast and powerful way to conduct risk assessments, plan secure routings, source freight crime metrics, and to identify TAPA-certified facilities, transport partners, and truck parking locations. I am confident you will soon appreciate the benefits it can bring to your supply chain resilience programmes.'

Thorsten Neumann,
TAPA EMEA



Incident Database
Access hundreds of thousands of cargo crime incidents

Map & Routing
Visualise risk and assess routes

Modus Operandi Analysis
Understand how criminals operate

Product & Loss Analysis
Identify targeted products and potential impact

Reports & Exports
Create, customise and export intelligence

24/7/365
ACCESS FOR TAPA MEMBERS

GLOBAL COVERAGE
Incidents from more than 160 countries worldwide.

TRUSTED NETWORK
Intelligence shared by members, authorities and partners.

TAPATRON

AI ASSISTANT

Your intelligent partner in cargo crime intelligence.

TAPATRON helps you find answers faster, uncover insights and make better security decisions.

Ask questions in natural language

Get answers using everyday language.

Get instant intelligence summaries

Receive quick overviews of trends, incidents and risks.

Explore trends and hotspots

Discover emerging threats and high-risk areas.

Save time. Make better decisions.

Intelligent support for faster, smarter actions.



STRONGER SECURITY

Better visibility. Lower risk. Safer supply chains.

ACTIONABLE INSIGHTS

Turn intelligence into action and stay one step ahead.

Securitas



Resilient by design

Turning TAPA standards into a living security system

Cargo crime has become a systemic risk to supply chain resilience and business continuity, and the organisations most exposed to it are increasingly judged, by clients, insurers and regulators alike, on their ability to demonstrate credible, auditable security controls. However, demonstrating compliance is only part of the picture. The real test is whether security stays effective as cargo moves between facilities, vehicles and rest stops across the whole journey.

"TAPA standards give the industry something essential: a common, auditable benchmark that clients and insurers can trust. But a standard describes a state, while security is a practice. The organisations that stay ahead treat compliance as the floor they build from, not the ceiling they aim for. They take the frameworks and make them operate continuously across the whole journey."

Morten Krohn Sommer Mikkelsen
Vice President Standardised Offering
Securitas Europe

From compliance to resilience

Dieter Blommaerts, Director Standardised Solutions, Securitas Europe, says, "Designing security into a supply chain means building an operating model that links intelligence, monitoring and response into a single system. We work with clients across the globe to design, implement and operate security programmes across the cargo journey. From that experience, we have identified four practical advantages of building a resilient, continuously operating security model."

Four practical advantages of building a resilient, continuously operating security model



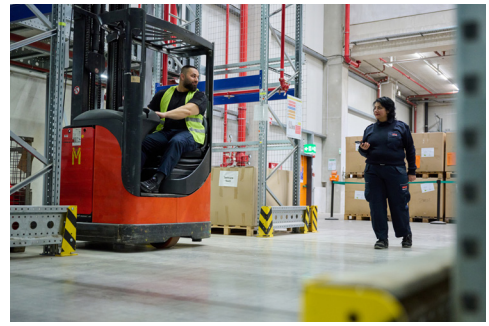
1 Maintaining visibility across the entire journey

Most transport operators have some form of vehicle tracking. Far fewer have connected that tracking to a monitoring framework capable of assessing signals in real time.

Blommaerts says, “The same question is relevant for most clients: if your trailer disconnects at 3 am, what happens next? In many cases, the honest answer is that they find out in the morning. That gap between an event and a response is where losses can occur.”

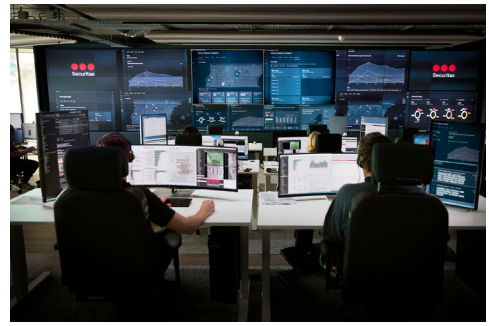
Securitas deploys a live monitoring architecture across client supply chains, managed through its global network of 24/7 Security Operations Centers (SOCs). Vehicles can be tracked using GPS, geofencing and sensors that detect door openings, trailer disconnections and route deviations.

At warehouses and parking hubs, the same discipline applies: access control, remote video analytics and active intrusion detection can be integrated to meet TAPA requirements and close blind spots across entry points, yards and internal zones.



2 Moving from reactive to preventive security

Effective security relies on turning intelligence into action. Through the Risk Intelligence Center (RIC) and SOC-led monitoring capabilities, Securitas can combine threat insight, incident data and location-based alerts to help clients understand changing risk conditions and make informed security decisions around route monitoring, secure parking, escalation protocols and response planning, aligned with each client’s risk profile and operational needs.



3 Protecting operational continuity

A compromised shipment sets off a chain of consequences: delayed deliveries, strained client relationships, insurance claims and the internal disruption of managing an incident without a plan. The value of visibility and intelligence lies in enabling a swift, coordinated response.

When the SOC verifies a threat, operators initiate immediate, pre-agreed procedures. These range from driver welfare checks and two-way voice communication to mobile patrol dispatch and direct coordination with local emergency services, underpinned by GPS positioning, panic alarms, man-down detection and mobile dispatch readiness.



4 Building security into client relationships

Mikkelsen says, “Security posture is one of the major deciding factors in many industry contracts. TAPA certification, combined with an integrated security model and a verified incident response capability, changes the commercial conversation. It moves security from a cost line to a competitive advantage.”

Built in, not bolted-on security

Securitas' security model can provide a TAPA-aligned security system, connecting people, technology and intelligence at every stage of the cargo journey.

FSR-ALIGNED

Protecting facilities

Warehouses, logistics hubs and distribution centres are naturally high-risk targets within the supply chain. Securitas designs and operates FSR-aligned security programmes combining:

- digital visitor management
- perimeter and internal video surveillance
- on-site guarding and mobile patrols
- centralised alarm handling
- fire, safety and emergency response

TSR-ALIGNED

Protecting movement

Road transport remains one of the most exposed stages of the supply chain. Securitas supports TSR-aligned operations through:

- 24/7 SOC monitoring and live vehicle tracking
- risk-informed routing using historical incident data
- driver protection combining emergency communication
- lone worker protection and welfare monitoring

PSR-ALIGNED

Protecting rest stops

Mandatory rest periods create some of the highest-risk windows in the entire cargo journey. Securitas supports PSR-compliant facilities through:

- controlled access and remote video surveillance
- SOC-led patrols and mobile patrol intervention
- lone worker protection
- historical incident intelligence and current threat data inform parking recommendations, reducing exposure during planned stops

Compliance is the foundation; resilience is what you build on it

Blommaerts says, "TAPA standards provide rigorous and effective frameworks. Our role is to make that framework operational, so that the standards are not just met on paper, but active at every stage of the journey."

The future of supply chain security will be defined by organisations that make the shift from security that proves compliance to security that delivers continuity.

Get in touch with our industry experts

Visit securitas.com



Dieter Blommaerts
Director Standardised Solutions
Securitas Europe

dieter.blommaerts@securitas.be
+32 474 701 584



Morten Krohn Sommer Mikkelsen
Vice President Standardised Offering
Securitas Europe

morten.mikkelsen@securitas.dk
+45 23 38 56 50



Supply chain security in Spain

REGISTRATION CLOSING SOON... **>100 DELEGATES ALREADY REGISTERED...**

TAPA EMEA REGIONAL CONFERENCE
Madrid – 21 October 2026

Over 18 months to the end of August 2026, the Transported Asset Protection Association (TAPA) recorded thousands of attacks on trucks, warehouses, and other types of facilities and modes of transport in Spain. The 13% of these cargo crimes reporting a loss value contributed to a total loss of goods in Spain of >€386 million.

Major losses (**€100K+**) of products in supply chain attacks in Spain averaged over **€1.3 million.**

Today, virtually all types of goods are a target for criminals in storage and in-transit, including...

- Metal
- Cash
- Tools & Building Materials
- Food & Drink
- Jewellery & Precious Metals
- Electronics
- Clothing & Footwear
- Cosmetics & Hygiene
- Phones
- Auto Parts
- Tobacco
- Agricultural Machinery
- Bicycles
- Furniture & Household Appliances
- Tyres
- Sports & Fitness Equipment
- Computers & Laptops
- Toys & Games
- Pharmaceuticals

What more can manufacturers and logistics service providers do to protect their supply chain operations in Spain from attacks by organised crime groups and other offenders?



ALL PANELS & PRESENTATIONS IN SPANISH

On **21 October 2026 in Madrid**, TAPA EMEA will bring together industry leaders and law enforcement agency professionals to look at the causes of freight crime in Spain as well as police work to disrupt crime groups. The event will also present proven security solutions already protecting supply chains across Europe, and the cargo crime incident intelligence driving this industry response.

Our conference is **free to join** but delegate places are limited, and only available on a first come, first served basis.

We invite you to join us in Madrid to learn more about protecting your supply chain in Spain and preventing the financial and reputational impact of a criminal attack.

TAPA EMEA members can register <u>one</u> delegate free of charge under their membership benefits. Additional delegate places cost €250.00 per person. Please note TAPA EMEA's *No-Show Policy* will apply to this event. Details on conference website.

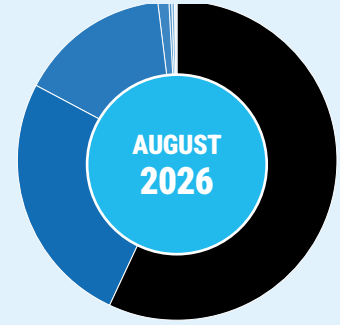
REGISTER NOW

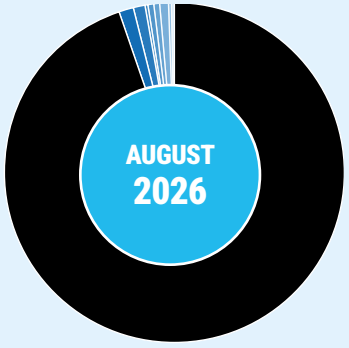
EUROPE, MIDDLE EAST & AFRICA REGION

CARGO CRIME MONITOR

€123,038,684

Total loss for the **347 or 1.5%** of crimes stating a value





LOCATION TYPE

Unknown	21,926	96.45%
Retail Store	329	1.45%
Origin Facility	253	1.11%
En Route	93	0.41%
Services 3rd Party Facility	79	0.35%
Railway Operation Facility	19	0.08%
Unclassified Parking	18	0.08%
Destination Facility	7	0.03%
Maritime Transportation Facility	3	0.01%
Secured Parking	3	0.01%
Road Transportation Facility	2	0.01%
Authorised 3rd Party Facility	1	0.004%

€1,313,950

Average loss for the **91** recorded cargo thefts with a value of **€100,000** or more reported to the TAPA EMEA Intelligence System (TIS) in August 2026

18

Crimes in EMEA recording a loss value of between **€50,000** & **€100,000**, totalling **€1,279,895**

21

Number of TAPA TIS product categories recording losses in August 2026

INCIDENT CATEGORY

Theft from Facility	12,730	56.00%
Theft	5,829	25.64%
Robbery	3,418	15.04%
Hijacking	394	1.73%
Theft from Vehicle	217	0.96%
Theft of Vehicle	40	0.18%
Theft of Trailer	29	0.13%
Theft from Trailer	24	0.11%
Counterfeit	21	0.09%
Truck Theft	16	0.07%
Theft from Container	7	0.03%
Fraud	3	0.01%
Theft from Train	2	0.01%
Clandestine	2	0.01%
Theft of Container	1	0.004%

70.2%

Or **15,969** of the reported incidents stated an M.O. of Violent or Threat with Violence

1,077

Number of new cargo crimes reported to the TIS database in August 2026

€354,578

Average loss for all cargo crimes reported with a value

€70,000,000

BIGGEST REPORTED LOSS IN AUGUST 2026: The seizure of counterfeit goods - some 160,000 packs of chewing tobacco - and banknotes in a police operation at an Origin Facility in Northern Algeria.

CARGO THEFT BY COUNTRY

65 Number of countries in EMEA reporting incidents

AUGUST 2026

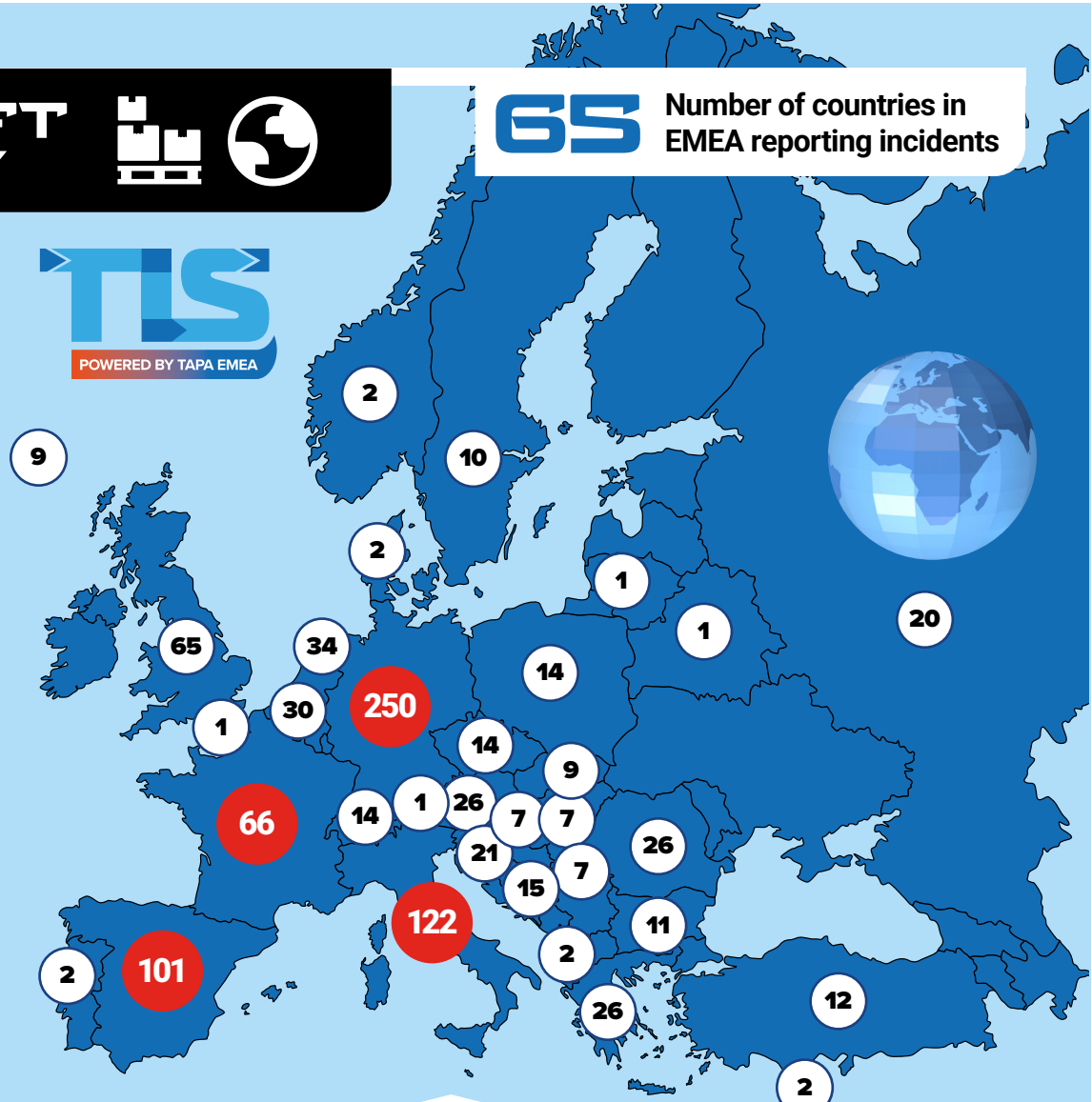
TOP 5	
South Africa	21,611
Germany	250
Italy	122
Spain	101
France	66

Rest of EMEA	
United Kingdom	65
Zambia	37
Belgium	34
Zimbabwe	31
Netherlands	30
Romania	26
Greece	26
Austria	26
Kenya	24
Croatia	21
Russian Federation	20
Bosnia and Herzegovina	15
Poland	14
Czechia	14
Switzerland	14
Azerbaijan	12
Turkey	12
Bulgaria	11
Sweden	10
Senegal	10
Botswana	9
Iceland	9
Slovakia	9
Morocco	9
Egypt	8

Rest of EMEA	
Kazakhstan	7
Slovenia	7
Hungary	7
Serbia	7
Nigeria	5
Kuwait	4
Madagascar	4
Oman	3
Mozambique	3
Yemen	3
Cyprus	2
Mauritius	2
United Arab Emirates	2
Benin	2
Portugal	2
Jordan	2
Cameroon	2
Norway	2
Denmark	2
Cote d'Ivoire	2
Montenegro	2
Mali	2
Eswatini	1
Niger	1
Jersey	1
Belarus	1
Mayotte	1
Somalia	1
Lebanon	1
Malawi	1
Algeria	1
Ghana	1
Iran	1
Liechtenstein	1
Lithuania	1

TOTAL RECORDED INCIDENTS: 22,733

TLS POWERED BY TAPA EMEA





DAILY LOSS FOR INCIDENTS REPORTED IN AUGUST 2026

€3,968,989

MODUS OPERANDI USED IN LATEST CARGO THEFTS:

Violent & Threat with Violence	15,969	70.25%
Unknown	5,869	25.82%
Intrusion	832	3.66%
Deception Other	30	0.13%
Internal	18	0.08%
Deceptive Pick Up	12	0.05%
Theft from Moving Vehicle	2	0.01%
Deceptive Stop	1	0.004%



Set the standard with TAPA. Go beyond it with Axis.

The threats you need to stop don't wait at the fence line.

TAPA FSR builds a strong security foundation. Axis takes you further. Radars and thermal cameras detect what's approaching beyond the fence line; GDPR-safe, in any light or weather. Horn speakers tell intruders they've been seen, ending incidents before they begin. License plate recognition and intercoms verify vehicles and drivers at access points, without staffing a gatehouse. On rooftops, radars detect presence before a skylight is ever breached. Axis: See further. Act sooner. Secure more.

For more information, please visit:
to.axis.com/tapa-emea-2026

AXIS COMMUNICATIONS

FAKE NEWS



Counterfeit goods are hitting supply chains hard, adding to freight crime concerns as cargo thieves cause tens of millions of euros in losses across 54 countries in EMEA in August…

Counterfeit goods have a devasting impact on businesses and national economies, especially in Europe. The fact that these fake products also need to move through supply chains, both legitimate chains where the authenticity of products is misrepresented and illegitimate transportation channels, very clearly makes this a formidable form of freight crime.

This is why TAPA EMEA added a specific 'Counterfeit' goods incident category to its database two years ago to make these types of crimes easier for member companies to identify.

Counterfeit goods are now said to cost European Union businesses over **€80 billion** in direct sales annually – a figure some industry insiders might consider conservative.

The European Union Intellectual Property Office (EUIPO) has previously highlighted the cost impact on specific industry sectors, which includes...

- **€12 billion** cost to the clothing industry



- **€3 billion** impact on genuine cosmetics sales



- **€1 billion** from the sale of counterfeit toys



In addition, counterfeit and illicit tobacco – said to represent over 41 billion cigarettes or about 10% of the market consumption - costs the European Union an estimated **€16.7 billion** in lost tax revenues annually.



And as EUIPO has reported: 'Besides economic losses and job impacts … counterfeiting fuels organised crime, undermines the trust in the rule of law and negatively affects the environment. Furthermore, counterfeiting in the cosmetics and toy sectors poses significant health and safety risks to consumers. These harmful products represent 15 % of counterfeit articles seized at the EU's borders." Other key sectors with safety concerns linked to counterfeit goods include automotive, electronics, and pharmaceuticals.

Furthermore, counterfeit goods – which reportedly account for approximately 5.8% of all imports entering the EU – put hundreds of thousands of jobs at risk across Europe.

This threat is highlighted in the latest freight crime reports to the TAPA Intelligence System (TIS). The top 3 incidents occurring in August by value all involved counterfeit goods:

- **€70 million** – the seizure of a major consignment of counterfeit chewing tobacco and banknotes from a facility in Northern Algeria on 24 August.
- **€8 million** – over 80,000 counterfeit products recovered from a warehouse in Burgos, Castile and León in Spain, on 5 August, including sportswear, shoes, 500 handbags, and 1,300 high-end watches.



- **€1,969,200** – a man was arrested after police found 5,000 items of counterfeit clothing, bags, wallets, and belts at a facility in Kotor in Montenegro.



Freight crime statistics added to the TIS database in August were heavily impacted by the addition of 15 months of cargo and

CONTINUED ON PAGE 29 >

MULTIPROTEXION
Powered by SCUTUM

OUR WEB SITE IS GOING TO CHANGE!

From January 2027 you will find us on
www.scutum-group.com

ABOUT MULTIPROTEXION

Since 1992, Multiprotexion has been one of the leading players in Europe in the active protection of high-risk goods in transit.

A great new journey called **Scutum Italia**.

Multiprotexion's journey began 34 years ago in Italy as a small company providing specialised services to the transport and building security sectors. Over the years, its solutions have become increasingly sophisticated, earning international recognition for their quality and high level of protection.
At the end of 2026, Multiprotexion will reach a major milestone as it becomes **Scutum Italia**, joining an international group united under a single brand.

This growth trajectory has led to a revamp of the company's brand image and the adoption of a new logo from the end of 2026.

The new identity reflects a shared commitment to delivering consistently high standards across all markets, while expanding our portfolio of technology-driven solutions to serve our customers even better. Scutum Italia will bring together the same trusted people and values under **a powerful new name** supported by broader expertise and the capabilities of an international group.

MULTI PROTEXION
PREDICTIVE SECURITY & TELEMATICS

1992 - 2025

MULTIPROTEXION
Powered by SCUTUM

2026

SCUTUM
ITALIA

2027

supply chain crime data made available by the South African Police Services (SAPS) for a week to March 2026. This intelligence includes truck hijackings, robberies at commercial sites, cash-in-transit robberies, and retail stock thefts.

As previously communicated, data reported in each issue of ***Vigilant***, covers (1) freight crimes that **occurred** in the previous month as well as incidents **reported** to TAPA EMEA in this same month, but which relate to earlier cargo thefts. All of this data then becomes accessible to the Association's members to support their analysis of crime trends in specific geographies and on key national and cross-border transport routes.



The addition of SAPS' bulk data upload means a total of 22,733 freight and supply chain crime incidents were added to the TIS database during August, producing a collective loss of **€123,038,684** for the 347 or 1.5% of reports sharing financial value data. This higher-than-usual loss was obviously also driven by the substantial recovery of **€70m** of counterfeit goods in Algeria, as stated.

This single crime also had a big impact on the statistics for freight crimes which occurred in August.

TAPA EMEA gathered data on 803 new freight thefts in the 31 days of the calendar month. Other key stats for the month included:

- **€90,609,281** in confirmed financial losses
- Based on the **17.9%** of incidents sharing their loss value
- x25 major crimes (**€100K+**) produced an average loss of **€3,568,404**
- Daily loss for crimes occurring in August 2026 = **€2,922,880**

In August, based on reports directly to TAPA EMEA, incidents impacted supply chains in 54 countries, with the top five countries…

- **Germany** – 180 freight crimes, 22.4% of the monthly total
- **South Africa** – 95 or 11.8%
- **Italy** – 83 or 10.3%
- **Spain** – 71 or 8.8%
- **France** – 48 or 5.9%.



Another 13 countries reported double-digit incident rates in August: United Kingdom (45), Zambia (29), Netherlands (25), Belgium (23), Zimbabwe (20), Greece (17), Croatia (15), Kenya (14), Switzerland (11), and 10 incidents each in Bosnia & Herzegovina, Botswana, Bulgaria, and Russia.

Whilst most freight crime reports to TIS in August did not specify the type of goods targeted, losses were still recorded in 20 TIS product categories, led by 102 cases of Fuel thefts and another 11 categories with double-digit incident rates…

- **Cash** – 60 robberies
- **Metal** – 50 crimes
- **Tools/Building Materials** – 44 reports
- **No Load** (Theft of truck and/or trailer) - 38
- **Jewellery/Precious Metal** – 36
- **Food & Drink** – 34
- **Computers/Laptops** – 29
- **Cosmetics & Hygiene** – 23
- **Miscellaneous Electronics** – 15
- **Tobacco** – 14
- **Phones** – 11

Major cargo thefts so far recorded in August include…



- **€1,241,850** – a cash-in-transit robbery in the Olomouc region of Czechia, on 13 August.
- **€1,000,000** – another theft of cash, this time targeting an armoured vehicle in Berlin, Germany, on 20 August.
- **€1,000,000** – server equipment stolen from trucks in Herzberg am Harez in Lower Saxony, Germany, on 30 August.
- **€968,162** – miscellaneous goods taken from a vehicle in Johannesburg, South Africa, on 7 August.
- **€900,000** – the recovery of 10 tonnes of halocarbon products en route in Kipoi in the Zagori region of Greece, on 9 August.
- **€600,000** – a driver was arrested after trying to use deception to pick-up a shipment of cognac from an Origin Facility in Charente, southwestern France, on 21 August.



- **€600,000** – jewellery/ precious metals were stolen during a robbery of a Retail Store in Paris, France, on 26 August.



- **€477,000** – police arrested a man for stealing a trailer and its load of miscellaneous products on 18 August in South Africa's Mpumalanga province.
- **€400,000** – four people were detained in connection with thefts of goods from four vehicles in Valencia, Spain, on 7 August.
- **€372,600** – a violent truck hijacking in Devon, Gauteng province, South Africa, on 19 August. The goods targeted were not recorded.
- **€320,000** – another violent robbery, targeting a cash-in-transit vehicle in Budva, Montenegro, on 9 August.
- **€300,000** – police in Tamworth in the UK Midlands arrested a man on 10 August in connection with the theft of copper from an Origin Facility.



- **€150,000** – another case targeting metal, on this occasion copper cable from a Services 3rd Party Facility on 5 August in Ginsheim-Gustavsburg in Hesse, Germany.
- **€111,291** – a Deceptive Pick-up crime involving a carrier sourced via an online freight exchange, which impersonated a transport provider known to the principal contractor. The driver and vehicle escaped with a load of Californian almonds from an Authorised 3rd Party Facility in Ridderkerk, Netherlands, on 5 August.



- **€100,000** – on 6 August, offenders stole gold chains from a jewellery retailer in Liskeard in the southwest of the United Kingdom.
- **€100,000** – 5 men were arrested after attempting to steal cosmetics from an Origin Facility warehouse in Majadahonda, Madrid, Spain.



- **€100,000** – tools/building materials were stolen from a Services 3rd Party Facility in Meerane, Saxony, Germany, on 19 August.
- **€100,000** – on 12 August, thieves stole bicycles from a Retail Store in Gap, France.

CONTINUED ON PAGE 31 >


Avertic®
Armour BY ENGTEX
ANTI-CUT PANELS THAT
STOP POWER TOOLS
Secure your high-value transports with
our anti-cut panels designed to stop break-in
attempts using power tools.
www.averticarmour.com

Due to a high number of recorded crimes in August not stating their loss value, TIS collated only nine incidents with losses of goods between €50K-€100K and these included…

- **€80,000** – toy cars stolen from a Retail Store in France, on 13 August.
- **€73,739** – smartphones, tablets, and smartwatches taken from a Retail Store in Yessentuki, Russia, on 13 August.



- **€71,433** – two men were arrested for stealing copper wire from an Origin Facility in Las Palmas, Spain, on 18 August.
- **€71,393** – 54,00 litres of fuel were stolen in Tema, Ghana, on 20 August. Two men were later arrested.

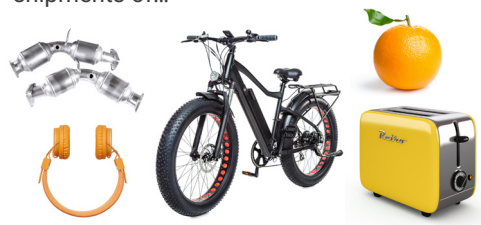


- **€60,000** – 15 bicycles were taken from a Retail Store in Saint-Galmier in Eastern France, on 13 August.
- **€60,000** – on 28 August, a consignment of drinks was stolen from an Origin Facility warehouse in Castile and León, Spain.



Over the course of the month, TIS also recorded the theft of 1,320 laptops from a truck left in an unclassified parking location in Heimsheim in Baden-Württemberg, Germany, as well as 440 air conditioning units stolen from a facility in Gretz-Armainvilliers during the height of the summer heatwave. In a separate incident in Spain, 40 aircon units and 25 water heaters were taken from an Origin Facility in Espinosa de los Monteros.

As if to highlight the diverse nature of freight crime in the Europe, Middle East & Africa region, during the month of August, TAPA EMEA also recorded losses of shipments of…



- Beer
- Brakes
- Catalytic converters
- Chainsaws
- Chocolate bars
- Chrome wheels
- Cider
- Cigarettes
- Coffee beans
- E-bikes
- Fabric rolls
- Gaming consoles
- Glasses
- Groceries
- Handbags
- Headphones
- Household Appliances
- Jigsaw puzzles
- LED facemasks
- Medication
- Motorcycles
- Oranges
- Perfume
- Pesticides
- Sausages
- Shampoo
- Shirts
- Shoes
- Socks
- Soya
- Tiles
- Toasters
- Toys
- Whiskey
- Wines

TAPA EMEA members can see all the latest freight crime data from across the EMEA region by logging into the TAPA Intelligence System (TIS).

Report freight thefts to us at **tisteam@tapaemea.org**

TIS POWERED BY TAPA EMEA

STOLEN PRODUCTS	No.	%
TOP FIVE		
Unspecified	21,581	94.93%
Miscellaneous	411	1.81%
Fuel Theft	131	0.58%
Metal	130	0.57%
Cash	87	0.38%
TOP FIVE TOTAL	22,340	98.27%
Tools/Building Materials	56	
Jewellery/Precious Metals	55	
No Load (Theft of truck and/or trailer)	45	
Food & Drink	42	
Clothing & Footwear	35	
Cosmetics & Hygiene	32	
Miscellaneous Electronics	22	
Phones	19	
Tobacco	17	
Bicycles/Two Wheelers	15	
Auto parts	12	
Toys/Games	9	
Tyres	9	
Furniture/Household Appliances	7	
Computers/Laptops	6	
Pharmaceuticals	6	
Agricultural Materials	4	
Sports & Fitness Equipment	2	
OTHER PRODUCTS	393	1.73%

DON'T FORGET TO TELL TIS..

When you see a media report about a cargo crime in your country, please copy the link and share this valuable intelligence with **tisteam@tapaemea.org**



SENSOS

ADVERTORIAL

Stop chipping away at the gap. Close it.

Supply chain leaders know cargo theft is a problem. Few realize it already has a solve.



A primary target for in-transit theft

Organised crime rings are getting smarter, faster, and more brash, and thieves know exactly how to exploit the gaps most operations still have. What far fewer leaders know is that the problem already has a solve.

Most security teams respond by refining what they already have — tightening a process, adding a checkpoint, buying a platform to watch one more data point. That chips away at the gap. It doesn't close it. And while security teams chip away, organised crime isn't standing still — it's running further ahead.

The answer is technology, specifically AI supply chain services that act when something goes wrong instead of simply raising an alert and waiting for someone to notice it. The outcome, not the notification, is the point.

"Visibility without a fast, structured response is not security. It is documentation."

That tends to make people nervous, and it should be questioned rather than waved away. But the real choice was never a machine acting alone versus a person. It's a system that decides in seconds, with a person still watching, versus a person deciding twenty minutes too late — if they see the alert at all.

THE GAP IS NOT DETECTION. IT'S EVERYTHING AFTER.

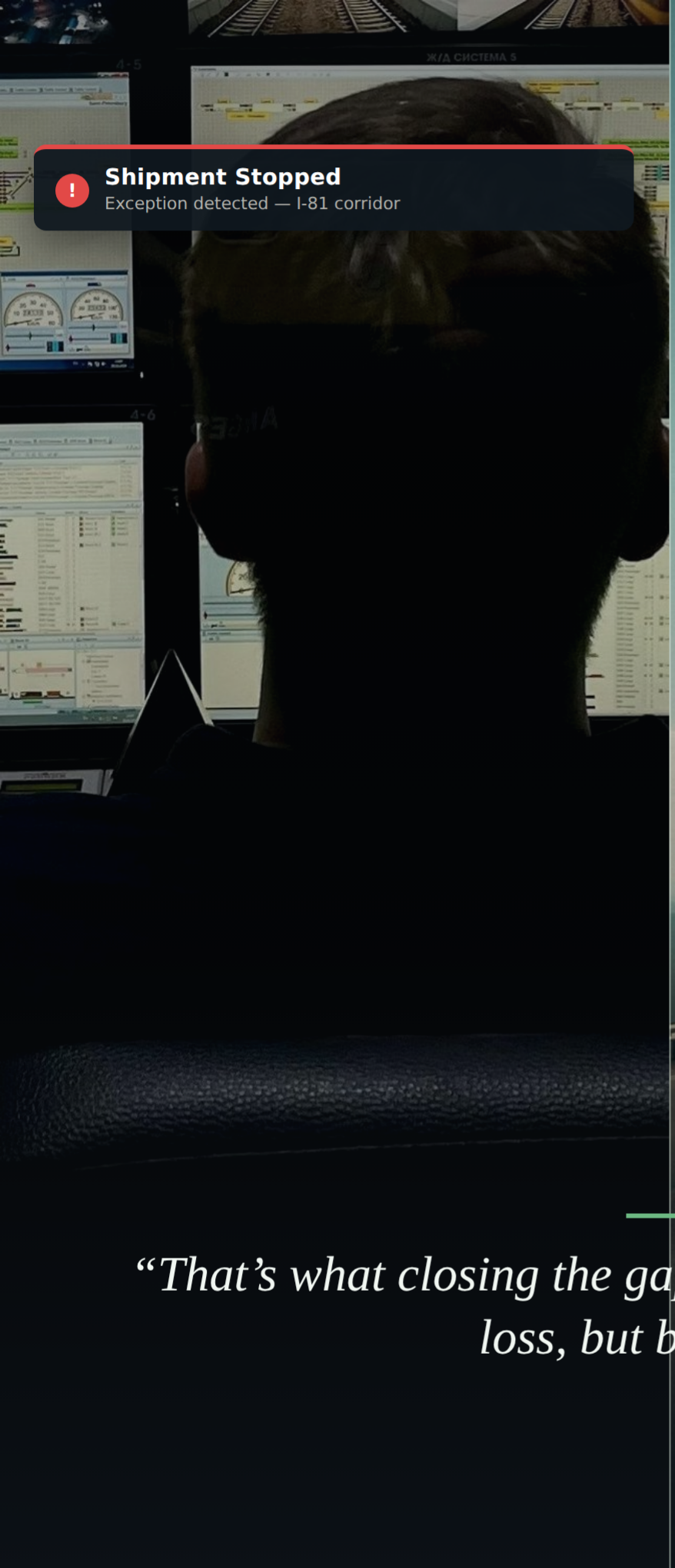
Visibility has genuinely improved over the past decade — tracking devices, geofencing, and carrier data integration all give today's shipper more situational awareness than before. *But visibility without a fast, structured response is not security. It is documentation.* Security teams have the alert and the data, but still can not act quickly enough. Too many steps, too many handoffs, too many decisions made with incomplete information. By the time a coherent picture is assembled, the window has closed.

Organised crime groups exploit this gap and move fast. In transit attacks, the entire job — doors opened, goods transferred, vehicles dispersed — can be finished in under ten minutes. A response chain that takes twenty minutes to mobilise was never in the fight.

Most tracking infrastructure is attached to the vehicle, not the goods. The moment they separate — as in roll-over attacks, where cargo is pulled through the roof or rear doors of a moving lorry — every piece of vehicle-based intelligence becomes irrelevant.

Law enforcement calls this their primary intelligence gap: they know a theft occurred, roughly where and when, but the trail ends there, and evidence stops cold at the point of transfer.

Gali Belleli · Head of Sales Development, Sensos





"That's what closing the gap looks like — not after the loss, but before it."

SENSOS

CONTINUED ON PAGE 34 >

SENSOS



Now, the question is: how fast can an organisation put an execution layer in place, and can that happen before the next significant loss?

AI that acts. Not just alerts.

Security is shifting from response to execution — from assembling information and deciding what to do, to infrastructure where the response logic is already defined, authorised, and ready to fire the moment conditions are met, without depending on a person being available at the exact right moment.

Sensos is built for exactly that. When something goes wrong, it detects the exception, decides what should happen next, and resolves it — automatically, or by putting it in front of a person. The logic exists before the incident does. The human role shifts from initiating the response to overseeing it — the practical effect is speed, not marginal but orders-of-magnitude speed.

That decision is only as good as the information behind it. A physical signal from the goods confirms what's actually happening; the carrier record reports what's supposed to be happening. Together, they close the gap — and the intelligence deepens over time, learning from what's played out across the industry so it can flag a problem before it repeats.

Contact Gali Belleli. galib@sensos.io

Gali Belleli · Head of Sales Development, Sensos



ARE YOU TUNED INTO OUR *TAPA TALKS* PODCAST...

PODCAST

Episode 4

of our *TAPA TALKS* Podcast is out on 2 October 2026.

In this new episode, TAPA EMEA's President & CEO, Thorsten Neumann, talks to co-host Sam Pauly about how our industry Association is changing behind the scenes to make it more efficient, to deliver new membership benefits, and how enhanced technology is optimising membership management processes, allowing our full-time resources to focus their time in areas that bring most value to the Association and its members.

You can download *TAPA TALKS* wherever you get your apps...

- Spotify
- Amazon Music
- Apple

... and listen via TAPA EMEA's YouTube channel.

Plus, you can still listen to our first three episodes, which include conversations with TAPA EMEA's Chair, Marcel Saarloos, and Vice Chair, Antonio Knezevic, as well as, in Episode 3, a special look at *'Fighting freight fraud & fake carriers'* as we were joined in the *TAPA TALKS* studio by Matt Arendas, Vice President, Partnerships at Trans.eu, the digital logistics ecosystem serving more than 44,000 verified transport partners, forwarders, and shippers across Europe.

DOWNLOAD *TAPA TALKS* NOW... JOIN THE CONVERSATION... & STAY TAPARIZED...

TAPA EMEA
Transported Asset Protection Association

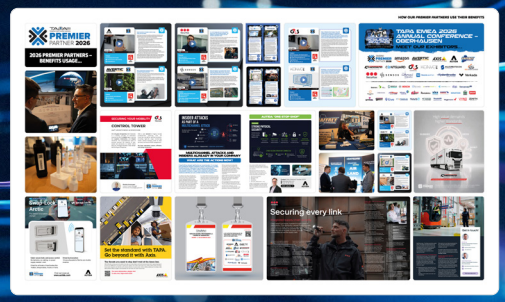
PREMIER PARTNER 2027

ARE YOU READY TO BECOME A *2027 PREMIER PARTNER?*



TAPA EMEA's *2027 Premier Partner* programme will open in October 2026 for elite providers of supply chain security products & services. If you want to enjoy the programme's unique 12-months of unique benefits to showcase your solutions to TAPA EMEA's network of decision-makers, buyers, and users of security product and services across 2027, please contact Thorsten.Neumann@tapaemea.org for more information...











PARTNERS IN SUPPLY CHAIN RESILIENCE

2027 PREMIER PARTNER BENEFITS INCLUDE...

- 12 MONTHS BRAND AWARENESS
- CONFERENCE VIDEO PROMO
- EXTRA CONFERENCE DELEGATE PASSES
- TARGETED ADVERTORIALS
- EXHIBITION SPACE
- ADDITIONAL DELEGATE PLACE DISCOUNTS
- 12-MONTH WEB PROFILE & VIDEO
- TARGETED ADVERTISING
- WEBINAR HOSTING
- SOCIAL MEDIA RECOGNITION





SOUTH AFRICA'S FREIGHT CRIME CHALLENGE

Why Intelligence, Standards & Local Adaptation Must Work Together...

South Africa is one of the most complex freight security environments in the TAPA EMEA region.

On one hand, we have world-class manufacturers, logistics providers, retailers, ports, roadfreight operators and private security capability. On the other hand, these supply chains operate in a threat environment where violent crime, organised criminal networks, infrastructure theft, illicit markets, and economic pressure all come together.

For companies moving goods in South Africa, freight crime is not an occasional abnormality. It is part of the operating environment and must be actively managed every day. The issue is not only that cargo is stolen. The issue is that freight crime in South Africa often involves violence, intelligence gathering, insider facilitation, fast disposal networks, and, very often, a highly developed private security response.

That makes South Africa different from many European markets. In Europe, a large share of cargo crime is linked to theft from vehicles, insecure parking, fraudulent carriers, and attacks on trailers. Those risks exist here too. But in South Africa, they sit alongside a more violent reality, where hijacking, armed robbery, fake authority stops, truck diversion, and attacks on last-mile delivery vehicles are part of the regular risk picture.



Where the risk is concentrated

Gauteng remains the most important and prolific freight crime hotspot in South Africa. That is not surprising. Gauteng is the country's economic engine and contains the largest concentration of distribution centres, warehouses, retail networks, courier operations, and, therefore, high-value cargo movements. It also connects directly into the N3 corridor to Durban, the N4 toward Mpumalanga and Mozambique, the N1 north and south, and the N12/N17 freight routes across the industrial belt.

That concentration is clearly visible in the reported hijacking figures. In the most recent provincial breakdown available, Gauteng accounted for 223 of South Africa's 349 truck hijackings, or roughly 64% of the national total. Within Gauteng, the areas around Ekurhuleni, Germiston, Kempton Park, Alberton, the East Rand, City Deep, the R21, N3 approaches and the broader Johannesburg–Pretoria logistics belt are especially important from a cargo security perspective. Public reporting has also highlighted Gauteng's dominance in truck hijacking hotspots, including a report that 25 of South Africa's top 30 truck hijacking hotspots were in Gauteng.

A recent two-week snapshot from TAPA EMEA's Intelligence System shows how broad that exposure is. Between 24 August and 6 September 2026, TIS recorded 47 incidents in South Africa. Gauteng appears repeatedly, with incidents recorded in Johannesburg, Pretoria, Mamelodi, Boksburg, Krugersdorp, Tembisa and Sedibeng, as well as incidents recorded more generally against Gauteng. But the same data also includes Durban, KwaMashu, Pietermaritzburg, Musina, Gqeberha, Mthatha, Secunda, Rustenburg, Brits, Verulam and other locations.

So, while Gauteng is the centre of gravity, this is not only a Gauteng problem.

The N3 Gauteng–Durban corridor remains one of the country's most critical freight arteries. It links South Africa's largest inland market to the port of Durban. That creates a predictable and high-volume flow of containers, FMCG, electronics, pharmaceuticals, clothing, automotive parts and other attractive cargo. The N4 corridor is similarly important, particularly for mining, fuel, bulk commodities, and cross-border trade. The N1 toward Limpopo and Beitbridge is also strategically important because of its cross-border exposure.

Freight crime in South Africa is also not confined to long-haul trucks. Attacks on Last Mile deliveries are also a major concern. Courier vehicles can carry multiple parcels, often including phones, electronics, clothing, pharmaceuticals, and other easily disposable goods. A single courier vehicle may not carry the same value as a full truckload, but its cargo is liquid, divisible, and easy to move through informal resale channels. That makes courier fleets attractive targets.

CONTINUED ON PAGE 40 >





The same 14-day TIS period shows how varied the incidents are. The 47 incidents included 12 hijackings, 12 robberies, 11 thefts from vehicles, four thefts from facilities and four counterfeit incidents, alongside thefts of vehicles and other forms of theft. The cargo categories were just as varied: cash, metals, fuel, electronics, food and drink, clothing and footwear, pharmaceuticals, and miscellaneous goods all appeared in the data.

Retail stores are also highly exposed, especially where criminals target high-value goods already close to the consumer market. Attacks on manufacturer and logistics warehouses do occur, but higher levels of access control, CCTV, guards, alarms, and armed response can make these premises harder targets. That does not mean facilities are safe. It means criminals will often attack the weakest point in the chain. In many South African cases, that is the vehicle, the driver, the road environment, the handover process or the last-mile route.

Modus operandi: old methods and new variations

The classic South African freight crime method remains armed hijacking. Trucks are intercepted by multiple suspects, often in more than one vehicle. The driver is threatened, removed from the vehicle or forced to comply. The cargo may then be offloaded, the trailer separated, the vehicle abandoned - or the entire unit moved to another location.

Violence runs through much of the recent intelligence. Of the 47 incidents recorded between 24 August and 6 September, 26 were classified as involving violence or the threat of violence. All 12 hijackings fell into this category. Violent incidents were also recorded as robberies and thefts from vehicles.

The detail matters. In only that short period, hijackings involved food and drink in Johannesburg, electronics in Sedibeng, metal in Pretoria, and fuel in Durban, while several other hijackings involved unspecified or miscellaneous cargo or vehicles recorded with no load. Violent cash robberies also appeared repeatedly, including incidents in KwaMashu, Mamelodi, Brits, Bojanala, and Johannesburg. It is only a snapshot, but it shows how varied the operational threat can be in a short period of time.

Fake police or 'blue light' stops are another major concern. Criminals may use uniforms, lights, marked or semi-marked vehicles, or simply the appearance of authority to force a driver to stop. This is particularly dangerous in South Africa because drivers are conditioned to comply with law enforcement. If criminals can imitate authority, they can defeat many normal driver security procedures. Public reporting has documented cases involving suspects using metro police uniforms and arrests connected to 'blue light' truck hijackings.

> ***'For companies moving goods in South Africa, freight crime is not an occasional abnormality. It is part of the operating environment and must be actively managed every day.'***

Another common method is deception. Criminals may signal to a driver that a tyre on their truck is flat, that the load is loose, or that something is wrong with the vehicle. When the driver stops to inspect, the attack begins. I see this as physical social engineering. It works for the same reason phishing works in the digital environment: urgency, credibility, and a request to break normal procedure.

GPS jamming and tracker discovery are also part of the threat landscape. Criminals know that most commercial vehicles are tracked. In higher-value attacks, they may search for tracking units, jam signals or move cargo from a tracked asset to another vehicle. For that reason, security can no longer rely only on tractor tracking. High-risk loads increasingly need layered visibility: tractor, trailer, cargo, seal status, route deviation, jamming alerts, and immediate control room escalation.

Cargo diversion is another growing area of concern. In these cases, the truck may be legitimate, the driver may be legitimate, and the paperwork may appear normal, but the load is taken to the wrong destination or offloaded at an unauthorised site. This is especially relevant in bulk commodities -



fuel, coal, metals, and other cargo types where a receiving yard or buyer can form part of the criminal chain.

The role of organised crime

It would be a mistake to describe South African freight crime as mainly desperate individuals stealing to survive. Poverty and unemployment do create a pool of people who can be recruited into crime, and some frontline offenders may indeed be low-income individuals taking short-term risks for money. But the more serious freight crimes usually require organisation.

A truck hijacking needs intelligence. What is being moved? When is it leaving? Which route will it take? Is there tracking? Is there an escort? Where can the cargo be offloaded? Who will buy it? How quickly can it be broken up or reintroduced into the market?

That points to organised criminal groups, or at least organised criminal networks, behind many major incidents. Even when small groups carry out the physical attack, someone normally facilitates the disposal of the goods. Stolen diesel, copper, food, clothing, electronics or pharmaceuticals must go somewhere. The receiver network is often the real economic engine behind the crime.

The range of goods appearing in the records is worth noting. Within only 14 days, the recorded incidents included repeated fuel theft, metal theft, electronics, food and drink, clothing and footwear, and pharmaceuticals. Four incidents were classified as counterfeit activity, involving clothing and footwear in Johannesburg, pharmaceuticals in Musina, metal in Gqeberha, and an unspecified commodity in Pietermaritzburg. The data does not prove how these incidents were connected, or whether organised groups were behind them, but it does show the variety of goods appearing in the current intelligence picture.

'A truck hijacking needs intelligence. What is being moved? When is it leaving? Which route will it take? Is there tracking? Is there an escort? Where can the cargo be offloaded? Who will buy it? How quickly can it be broken up or reintroduced into the market?'

This is why industry should not only focus on the hijackers. We also need to focus on the market for stolen goods: scrapyards, informal traders, dishonest wholesalers, complicit warehouses, illicit fuel buyers, and cross-border disposal routes. Without receivers, cargo crime becomes much less profitable.

SAPS data and the real picture

South African Police Service (SAPS) data is important, but it does not show the full freight crime picture. Official police statistics are useful for tracking broad trends in truck hijacking, robbery, and related commercial crime categories. SAPS publishes quarterly and annual crime statistics, and these remain the formal national reference point.

However, the reality on the ground is broader than the SAPS categories. Freight crime includes hijacking, attempted hijacking, theft from vehicles, fraudulent collection, cargo diversion, facility theft, courier robbery, diesel theft, infrastructure theft, seal tampering, jamming, insider collusion, and illicit cargo being inserted into legitimate logistics networks.

The difference becomes visible when we look beyond hijacking as a single category. In the 24 August to 6 September TIS records, 12 incidents were classified as hijackings. Some involved cargo taken from vehicles or facilities; others involved robbery, fuel theft, counterfeit goods, vehicle theft or container theft. One metal theft on 29 August was recorded at a railway operation facility, while facility incidents occurred at origin and third-party facilities.

Not all these incidents are reported consistently. Some are handled privately by insurers, transporters, cargo owners, tracking companies, or private investigators. Some are reported to police but not classified in a way that makes them visible as "freight crime". Others never reach public reporting because South Africa has many other serious crime and political stories competing for attention.



CONTINUED ON PAGE 42 >

> ***'There is also a practical reporting gap. In some cases, companies report the event formally because they need a police case number for an insurance claim. In other cases, especially where the operator self-insures, where cargo is recovered quickly, or where the loss is handled privately, the incident may not enter a broader intelligence picture in a useful way.'***

There is also a practical reporting gap. In some cases, companies report the event formally because they need a police case number for an insurance claim. In other cases, especially where the operator self-insures, where cargo is recovered quickly, or where the loss is handled privately, the incident may not enter a broader intelligence picture in a useful way. That does not mean the incident did not happen. It means it may not be visible to the rest of the market.

This means the rest of EMEA probably does not have a full picture of the actual level of freight crime in South Africa.

Police, private security and enforcement

South African authorities do recognise that freight crime damages the economy and the country's business reputation. The challenge is visibility and capacity. Freight crime is a major issue for the transport, logistics, insurance, and retail sectors, but it does not always dominate the national news agenda in the way it might in Europe. South Africa faces many serious crime and infrastructure challenges at the same time.

Police do investigate freight crime, and there are successful arrests and recoveries. Specialist units, local detectives, highway patrols, border police, and other enforcement structures all play a role. However, in practice, private security is often the main driver of prevention, response, recovery, and arrest support.

This is one of the defining features of the South African environment. Armed escorts, private investigators, tracking companies, control rooms, armed response teams, and recovery units are deeply embedded in logistics security. Many transport operators rely on them because police resources are limited, and response times can vary.

The priority is always the safety of the driver. Because many attacks are violent, drivers are generally trained not to resist.

The security model therefore depends heavily on covert alerts, tracking, control room monitoring, route management, and rapid private response. In many cases, private security teams are the ones who find the vehicle, coordinate recovery, preserve evidence, and support police in making arrests.

When offenders are prosecuted, penalties can include jail time and fines, but for many lower-level offenders, imprisonment is the most common consequence. The harder challenge is reaching the organisers and receivers behind the frontline criminals.

> ***'Police do investigate freight crime, and there are successful arrests and recoveries. Specialist units, local detectives, highway patrols, border police, and other enforcement structures all play a role.'***

Security methods used by industry

South African businesses use a wide range of loss prevention methods. These include vehicle tracking, geofencing, route planning, driver vetting, panic buttons, covert alarms, cargo seals, armed escorts, chase vehicles, secure parking, high-risk route procedures, control room monitoring, and private recovery teams.

For high-risk cargo, escorts are common. This is different from many European environments and is one of the reasons why South Africa may need a local interpretation or addendum to global best practice. Security standards that work well in a lower-violence environment may need to be supplemented where armed attacks are a normal operational risk.

The most effective methods are layered. No single technology or procedure is enough. A tracker can be jammed. A driver can be deceived. A subcontractor can be compromised. A seal can be cut. A route can become predictable. Effective security combines intelligence, technology, people, and response.

The variety of incidents recorded over those 14 days also shows why those layers matter. Incidents occur en route, at origin facilities, at third-party facilities, around vehicles, and, in one case in the latest data, at a railway operation facility. Some involve intrusion, others deception, and a large proportion involve violence or the threat of violence. The controls required for one type of incident will not necessarily prevent another.

Businesses do not simply accept freight crime, but many do treat it as an occupational hazard that must be budgeted and managed. The danger of that





mindset is resignation. The opportunity is collaboration. Information sharing through TAPA EMEA can help the industry move from individual defence to collective intelligence.

Why TAPA EMEA uptake has been limited

TAPA EMEA has invested time and effort in South Africa, but membership and Standards' certifications have not yet reached the level one might expect given the scale of the threat.

One reason is that the strongest driver must come from cargo owners, manufacturers, shippers, and insurers. If the owner of the goods requires TAPA Standards, transporters will respond. If insurers recognise and reward TAPA-certified and aligned controls, adoption will accelerate. Without that pressure, many operators continue with their existing private security arrangements, even if those arrangements are not benchmarked against an international standard.

Another reason is that the South African operating environment has specific characteristics that are not always fully reflected in a Standard developed for a broader EMEA audience. In particular, South Africa's use of armed escorts, private response, and violent-attack protocols need to be recognised more explicitly. TAPA's TSR 2026 and FSR 2026 are now live, and TAPA's downloads include updated security requirements and guidance documents. The next step is to translate these into the South African environment in a practical way.

A South African supplement or best practice guide linked to TSR could help. It should not replace the TAPA Standard. It should explain how to apply it locally, especially for hijacking, armed escorts, private security, 'blue light' stops, jamming, driver safety, and high-risk route management.

What needs to happen next

To grow TAPA's presence in South Africa, three things are needed.

First, cargo owners and manufacturers must push adoption of the TAPA Standards. They have the commercial power to make standards matter. If they require TAPA-certified security from their transport and logistics providers, the market will move.

Second, insurers should be part of the conversation. Freight crime is an insurance issue as much as a logistics issue. If insurers support TAPA Standards through risk assessment, premium recognition, or claims analysis, adoption will become more attractive.

Third, South Africa needs stronger intelligence sharing. TAPA members should submit more data into TIS – which relies heavily of SAPS data currently - attend the quarterly working group meetings and share what is working and what is not. We cannot defeat organised freight crime through isolated company responses.

> ***'The launch of South Africa's National Truck Stop Framework is also important. This creates an opportunity for TAPA's Parking Security Requirements to support national thinking on secure truck parking.'***

The 47 incidents recorded in those 14 days are a good example of why that sharing matters. They span different crimes, goods, locations and points in the supply chain. The value of intelligence is not simply in counting incidents after they happen. It is in seeing patterns early enough for operators to respond.

The launch of South Africa's *National Truck Stop Framework* is also important. The framework is intended to standardise and improve truck stops, including security, along freight corridors. This creates an opportunity for TAPA's Parking Security Requirements to support national thinking on secure truck parking.

In October, we are planning to hold the next TAPA South Africa quarterly meeting. The aim is to bring current members together to discuss current trends and incidents, new prevention methods, information sharing and practical lessons from the market. Most importantly, we need to discuss how to grow the membership base.

The bigger the group, the stronger the intelligence picture. The stronger the intelligence picture, the better we become at disrupting the syndicates behind the crime.

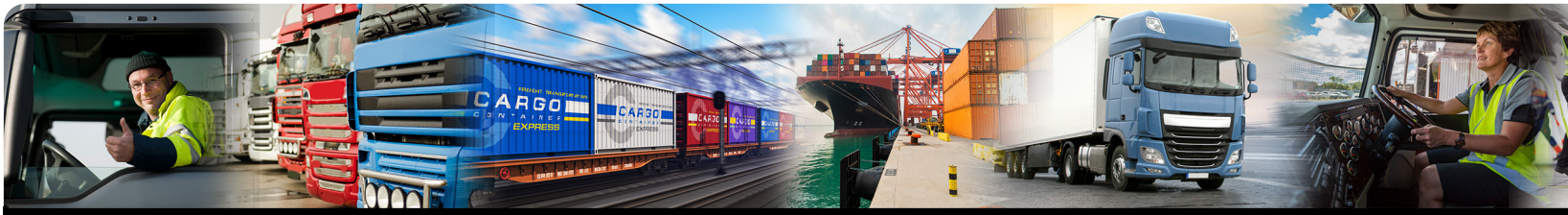
South Africa's freight-crime challenge is serious, but it is not hopeless. The country already has strong private security capability, experienced logistics operators and growing awareness of the economic damage caused by cargo crime. What is needed now is alignment: cargo owners, logistics providers, insurers, private security, law enforcement and TAPA EMEA working from the same intelligence picture and the same standards-based framework.

That is where TAPA EMEA can make a real difference.

Author profile:

Pieter Smits, TAPA EMEA's Regional Ambassador, South Africa, is CEO of Globaltrack, based in Johannesburg.





TAPA'S LATEST FSR, TSR & PSR STANDARDS' CERTIFICATIONS

SECURITY LEADERS

MONTHLY STATISTICS

TOTAL NUMBER OF CERTIFICATIONS
68

NUMBER OF COMPANIES CERTIFYING
32

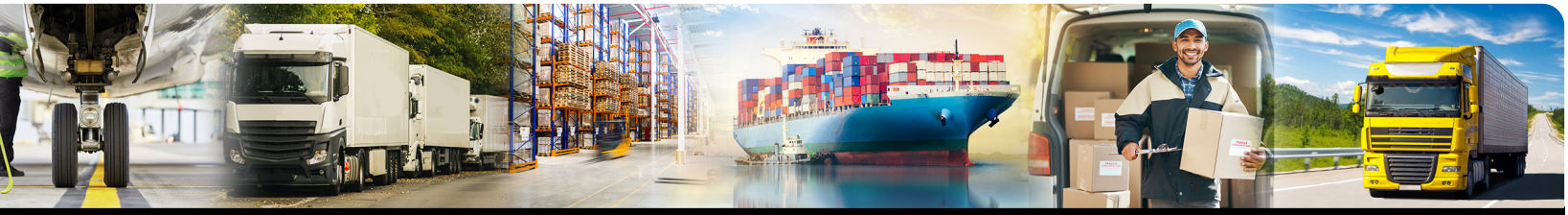
COUNTRIES IN EMEA RECORDING CERTIFICATIONS
22

TAPA EMEA
Transported Asset Protection Association

The following companies and locations were audited by one of TAPA EMEA's approved Independent Audit Bodies (IABs) or, in the case of Class 'C' or Level 3 certifications for FSR and TSR respectively, may have been completed by an in-house TAPA EMEA-trained person. Plus, a list of our latest PSR Partners and certifications.

FSR – EUROPE, MIDDLE EAST & AFRICA REGION

	COMPANY NAME	CITY	COUNTRY	CLASS
FSR	Amazon Com INC	Colleferro	Italy	A
FSR	Amazon Com INC	Fiano Romano	Italy	A
FSR	Amazon Com INC	Leeds	United Kingdom	A
FSR	Amazon Com INC	Leeds	United Kingdom	A
FSR	Amazon Com INC	Ardea	Italy	A
FSR	Amazon Com INC	Leeds	United Kingdom	A
FSR	Amazon Com INC	Jesi	Italy	A
FSR	Amazon Com INC	San Salvo	Italy	A
FSR	Amazon Com INC	Altrincham	United Kingdom	A
FSR	Amazon Com INC	Warrington	United Kingdom	A
FSR	Amazon Com INC	Bolton	United Kingdom	A
FSR	Amazon Com INC	Coventry	United Kingdom	A
FSR	Amazon Com INC	Redditch	United Kingdom	A
FSR	Amazon Com INC	Derby	United Kingdom	A
FSR	Amazon Com INC	Sutton-in-Ashfield	United Kingdom	A
FSR	Amazon Com INC	Sady	Poland	A
FSR	Amazon Com INC	Szczecin	Poland	A
FSR	Augustin Quehenberger Group GmbH	Fischamend	Austria	B
FSR	DHL Express	Besançon	France	C
FSR	DHL Express	Vitrolles	France	C
FSR	DHL Express	Dubai	United Arab Emirates	A
FSR	DHL Express	Sharjah	United Arab Emirates	A
FSR	DHL Express	Regensdorf	Switzerland	A
FSR	DHL Freight Germany Holding GmbH	Villingen-Schwenningen	Germany	C
FSR	DHL Freight Germany Holding GmbH	Ostersund	Sweden	C
FSR	DHL Freight Germany Holding GmbH	Maia	Portugal	C
FSR	DHL Global Forwarding Italy SPA	Sesto Fiorentino	Italy	C
FSR	DHL Management Switzerland Ltd	Budapest	Hungary	A
FSR	DSV A/S	Dubai	United Arab Emirates	A
FSR	DSV A/S	Pavlov	Czechia	C
FSR	FAN Courier Express SRL	Bucuresti	Romania	C
FSR	FIEGE Logistik Stiftung & Co. KG	Bellheim	Germany	C
FSR	Fiege Logistik Stiftung & Co. KG	Emmerich am Rhein	Germany	C
FSR	Geodis FF Germany & Co KG	Koln	Germany	C
FSR	Geodis FF Germany & Co KG	Rotterdam - Pernis	Netherlands	C
FSR	Geodis FF Germany & Co KG	Venlo	Netherlands	C
FSR	Geodis FF Germany & Co KG	Manchester	United Kingdom	C
FSR	Geodis FF Germany & Co KG	Aurach	Germany	C
FSR	Geodis FF Germany & Co KG	Rodgau	Germany	C
FSR	Geodis Sweden AB	Göteborg	Sweden	C
FSR	Gulf Drug LLC	Dubai	United Arab Emirates	C
FSR	Gulf Drug LLC	Abu Dhabi	United Arab Emirates	C
FSR	Gulf Drug LLC	Dubai	United Arab Emirates	C
FSR	Ingram Micro Europe b.v	Straubing	Germany	A
FSR	Ingram Micro Europe b.v.	Brwinow	Poland	C
FSR	Ingram Micro Europe b.v.	Cairo	Egypt	C
FSR	Naeko Logistics Group	Torrejon de Ardoz	Spain	A
FSR	Nippon Express Italia S.P.A.	Lainate	Italy	A
FSR	SMD Logistics AB	Kungsängen	Sweden	A
FSR	trans-o-flex Express GmbH & Co. KGaA	Westerkappeln	Germany	C



...HELPING TO IDENTIFY LEADERS IN SUPPLY CHAIN SECURITY



TSR – EUROPE, MIDDLE EAST & AFRICA REGION

	COMPANY NAME	COUNTRY	LEVEL
TSR	APM IKE - Magoula	Greece	Level 1 / Category - Small
TSR	Augustin Quehenberger Group GmbH - Fischamend-Dorf	Austria	Level 1 / Category - Small
TSR	BAR-NUL Kft - Szomód	Hungary	Level 1 / Category - Small
TSR	CEVA Logistics - Warszawa	Poland	Level 1 / Category - Small
TSR	DSV A/S - Riyadh	Saudi Arabia	Level 3 / Category - Large
TSR	Hannon Pharma Link Limited - Dublin	Ireland	Level 1,2 / Category - Medium
TSR	J&L autotrasporti srls - Trento	Italy	Level 1 / Category - Small
TSR	Nord Green Trans Kft. - Nyiregyhaza	Hungary	Level 1 / Category - Small
TSR	Nuova Express Line - Gricignano di Aversa	Italy	Level 1 / Category - Medium
TSR	Phone Express SAS - Olivet	France	Level 1,3 / Category - Small
TSR	Platform Uluslararası Taşımacılık Ticaret ve Sanayi Limited Şirketi - Antakya/Hatay	Turkey	Level 1 / Category - Small
TSR	Roissy Airport Express - Tremblay-en-France	France	Level 3 / Category - Small
TSR	Rozoti Prodcom SRL - Oradea	Romania	Level 3 / Category - Medium
TSR	Szaki Trans Kft. - Budapest	Hungary	Level 1 / Category - Medium
TSR	Transportes Sanchez Zarco E Hijos S.L. - Novelda	Spain	Level 2 / Category - Small
TSR	WES CT– LOG SAS - Louvres	France	Level 1 / Category - Small
TSR	Voge Transport Ltd - Crewe	United Kingdom	Level 1 / Category - Small

PSR/PPD – EUROPE, MIDDLE EAST & AFRICA REGION

	COMPANY NAME	CITY	COUNTRY	PSR / PPD
PSR/PPD	Batim Transport BV	Menen	Belgium	PPD
PSR/PPD	Fabb Park	Hauconcourt	France	PPD











TOTALLY TAPARIZED!

Every year, TAPA EMEA's work to support members using our supply chain security standards, the development of our training programme, the growth of our supply chain intelligence platform, and our networking events and security insights, are delivered with the support of our *Premier Partners*, all leading providers of supply chain security products and services – and all strongly committed to advancing the resilience of our members' supply chains.

We thank all our *2026 Premier Partners* for their support and for being TOTALLY TAPARIZED.

TAPA PREMIER PARTNER 2026 · amazon · AUTIDA · Avertic Armour BY ENGTEX · AXIS COMMUNICATIONS · CAFFREY INTERNATIONAL · HIGGINTO everywhere on the roads

CONTGUARD · G4S An Allied Universal Company · KONVOI · MULTIPROTEXION Powered by SCUTUM · SECOMPANION · Securitas

SENSOS · THECARGOSECURITY.COMPANY™ · TW TRUCK.WATCH · TydenBrooks SECURING THE WORLD · Verkada

ASK US HOW TO BECOME A *2027 PREMIER PARTNER* - CONTACT INFO@TAPAEMEA.ORG

PARTNERS IN SUPPLY CHAIN SECURITY & RESILIENCE