



FENESTRA TI

GLOBAL INTELLIGENCE. **CONNECTED INSIGHT.**

PANOPTIC — EXECUTIVE & VIP PROTECTION

PROTECTION STARTS WITH VISIBILITY

For executives, principals and the teams who protect them.

THREAT INTELLIGENCE HAS A SIGNAL PROBLEM

Most organisations aren't short of feeds — they're short of relevance. Generic OSINT dashboards surface thousands of alerts a week and leave security teams to work out which three actually matter.

Meanwhile the risks that do the damage rarely announce themselves in a single feed — a breached credential, a dark web mention, a hostile actor's shifting focus, and a principal's travel itinerary can each look unremarkable in isolation, and only make sense together.



Alert fatigue. Volume without prioritisation just moves the problem downstream.



Disconnected signals. Cyber, physical, and geopolitical risk are tracked in separate tools that never talk to each other.



Stale context. A pre-trip briefing or a quarterly risk report is out of date the moment circumstances change.

Fenestra was built to close that gap — fusing real-time collection with human analysis, so what reaches you isn't noise. It's a picture you can act on.

PERSONAL & DIGITAL EXPOSURE

THE PROFILE AN ATTACKER WOULD BUILD

Executives and high-profile individuals carry a different risk profile from the organisations they lead. Panoptic tracks personal exposure at the level an attacker would actually use.

Breached personal data — credentials, PII and accounts linked to the individual.

Residences & regular venues — crime and security events around the places they live and visit.

Dark web mentions — naming the individual or their inner circle.

Digital footprint — the same picture an attacker would build.

AI FINDINGS SUMMARY Generated 26/10/2026, 19:10:22 · based on 16107 findings

Unlimited AI Tokens [Regenerate](#)

PERSONAL DIGITAL-IDENTITY EXPOSURE

No dark-web identity exposure, credential leaks, or impersonation activity specific to Eleanor Vance (VIP self) was detected in this reporting period. Fenestra's tracked threat-actor data shows no targeting-relevance to Vance Holdings Ltd or its CEO role.

INNER-CIRCLE RISK

No findings concern family members, staff, or associates of the VIP. No inner-circle credential leaks, threats, or compromises are evident in the data.

RESIDENCE & ASSET PROTECTION

Geospatial findings for August 2026 cluster in London's West End (Leicester Square, Covent Garden, Theatre/Concert Hall, Strand, Trafalgar Square, shopping areas, nightclubs, and parking facilities), consistent with routine street crime rather than organized targeting. No threats to the monitored London Residence (51.5074, -0.1278 ±1km) are directly corroborated. Crime categories include theft from persons [H5, H12, H19, H26, H28, H33, H35, H40, H42, H47, H49], robbery [H20, H27, H34, H41], shoplifting [H7, H14, H21, H48], and violence/sexual offences [H1, H8, H15, H22, H29, H36, H43, H50]—typical of high-footfall leisure districts, not asset-specific threats.

PERSONAL-SECURITY RECOMMENDATIONS

- Vary personal routines and avoid predictable patterns in London residence and workplace travel.
- Maintain situational awareness in crowded venues (airports, shopping areas, theatres); keep valuables secured and monitored.
- Use hotel/venue concierge for secure transportation and pre-book ground transport rather than hailing taxis in high-crime areas.
- Establish check-in protocol with security team at start and end of each travel leg; confirm comms before and after airport transit.

Weekly assessment — identity exposure, inner circle, residence and personal-security recommendations for one principal.

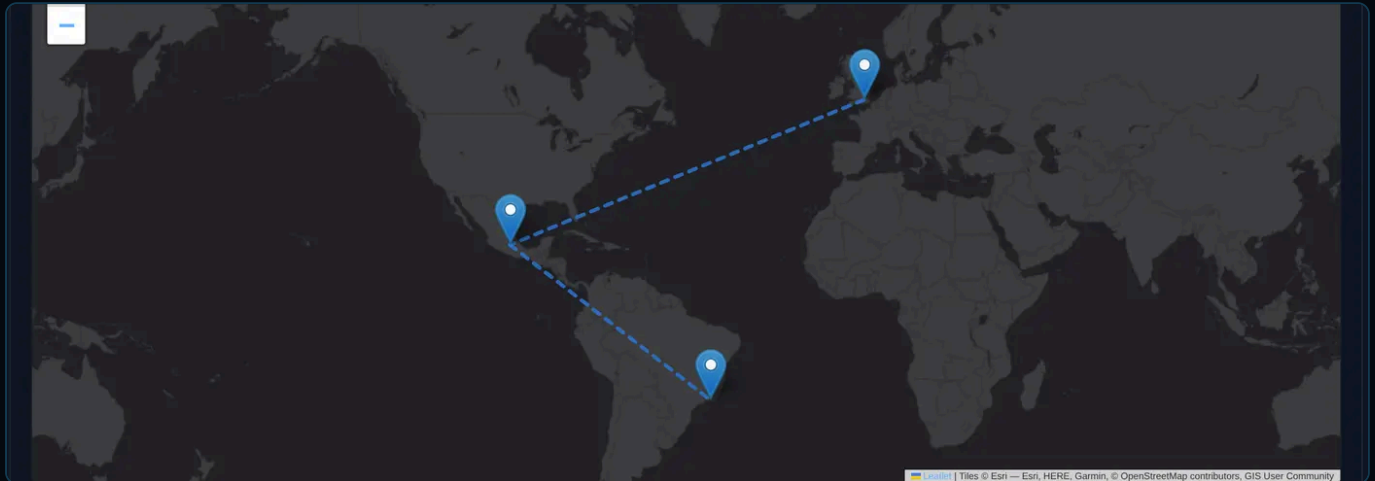
The result: a clear, individual risk picture built to inform close protection and executive security decisions — not just flag keywords.

Screens from the live Panoptic platform, using a demonstration profile for a fictional executive. Threat-actor, vulnerability and event data shown is real.

ITINERARY MONITORING

TRAVEL RISK THAT UPDATES AS FAST AS THE SITUATION

Every leg of a trip is checked against conflict, crime, aviation and cyber events around each stop — with live alerts as departure approaches, not a briefing that goes stale at take-off.



Route map — every monitored stop and leg of the itinerary.

LIVE TRAVEL ALERTS

3 high
4 medium
225 low

3 high-severity alerts near your travel — top: conflict near Rio de Janeiro - Galeão International Airport (GIG) (in 12d)

- Rio de Janeiro - Galeão International Airport (GIG)** (in 12d) — conflict · Conflict — Avenida Rei Pelé, Maracanã, Rio de Janeiro, Southeast Region, 20271-111, Brazil · Avenida Rei Pelé, Maracanã, Rio de Janeiro, Southeast Region, 20271-111, Brazil 2026-10-24 · 11.4km
- Rio de Janeiro - Galeão International Airport (GIG)** (in 12d) — conflict · Conflict — Rio de Janeiro, Southeast Region, Brazil · Rio de Janeiro, Southeast Region, Brazil 2026-10-26 · 12km
- Mexico City International Airport (MEX)** (in 8d) — cyber, crime · Cyber, Crime — Mexico City, Mexico · Mexico City, Mexico 2026-10-26 · 15.3km
- Rio de Janeiro - Galeão International Airport (GIG)** (in 12d) — crime · Crime — Rio de Janeiro, Southeast Region, Brazil · Rio de Janeiro, Southeast

Live travel alerts — ranked by severity, with how soon the principal reaches each stop and how close each event is.

Aviation notices — tracked against every airport and leg.

Cyber events — affecting airports, venues and local infrastructure.

Conflict & security incidents — near each stop, in real time.

Crime & unrest — around hotels, venues and transit points.

Screens from the live Panoptic platform, using a demonstration profile for a fictional executive. Threat-actor, vulnerability and event data shown is real.

ANALYSIS, NOT JUST ALERTS

A BRIEFING, NOT A FEED

Each itinerary gets its own written assessment: what the findings could mean for the trip, which groups are behind them, whether they are part of a wider pattern, and how a problem on one leg affects the next.

WEEKLY AI SUMMARY

Generated 26/10/2026, 19:20:12 · based on 200 findings

Unlimited AI Tokens [Regenerate](#)

Findings include a terrorism/conflict reference at Heathrow [H2], a ransomware threat to Airbus infrastructure in Mexico City [H3], multiple crime incidents in Rio de Janeiro [H5][H6][H7][H8], and extensive airport infrastructure closures (NOTAMs) at Mexico City International Airport. The UK leg shows minimal threat activity, while Mexico and Brazil legs face operational and security risks.

POTENTIAL IMPACT

Ransomware targeting critical Airbus radio networks in Mexico City could degrade airport communications and emergency services [H3]. Crime spikes and gang violence in Rio de Janeiro neighborhoods [H5][H6][H8] elevate ground-level security risks. Extensive runway and taxiway closures at Mexico City airport [H9–H200] may cause significant flight delays, missed connections, or rerouting.

THREAT GROUP RELATION

Comando Vermelho is tracked with 173 real recorded events near Rio de Janeiro. Gang violence documented in [H5][H6] aligns with this group's known activity pattern in those favelas, though the findings do not attribute specific incidents to them.

PART OF A WIDER THREAT?

The Brazil findings show a pattern: firearm discharges and gang celebrations [H6], bus arson [H7], and street robbery [H8] all on or near the same dates (2026-10-24 to 26), suggesting coordinated or opportunistic criminal activity rather than isolated incidents. Mexico City infrastructure disruptions span 6+ weeks of NOTAMs, indicating prolonged operational strain.

CROSS-IMPACT ON OTHER LEGS

If Mexico City airport capacity is severely constrained by runway/taxiway closures, onward connections to or from Rio de Janeiro may be delayed or missed. Cyber disruption to Airbus radio networks [H3] could cascade into ground handling delays affecting any aircraft transiting Mexico City, compounding the already extensive infrastructure closures.

Itinerary assessment — impact, threat-group context, wider patterns and knock-on effects across legs — refreshed as the situation changes.

Built for close protection and travel security teams who need to know what's changed since this morning — not just what was true last week.

Screens from the live Panoptic platform, using a demonstration profile for a fictional executive. Threat-actor, vulnerability and event data shown is real.

HOW YOU WORK WITH US

TWO WAYS TO WORK WITH FENESTRA

Same platform, same collection. You choose who drives it.

SELF-MANAGED

Your team runs Panoptic directly.

- Live dashboards and alerts across everything you monitor.
- Weekly AI-generated summaries and on-demand PDF reports.
- You decide what's monitored — principals, residences, itineraries and devices.

BEST FOR

Protection teams that want hands-on control of their monitoring.

ANALYST-MANAGED

Fenestra analysts run it on your behalf.

- Our analysts set up and tune your monitoring.
- Findings reviewed by an analyst before they reach you.
- Written assessments and briefings, with escalation when something needs action.

BEST FOR

Principals, family offices and executive offices that want it handled for them.

Either way, you get the same collection, the same platform and the same intelligence behind it.

WHY FENESTRA

BUILT ON REAL COLLECTION, NOT REPACKAGED FEEDS

Fenestra runs its own multi-source collection infrastructure — spanning global news, geopolitical event data, dark web, breach data, and cyber threat reporting.

Genuine breadth of collection — not a single-vendor feed reseller.

Analysts behind the intelligence — every actor profile and assessment shaped by analysts, and on your account if you want them.

Fused, not siloed — cyber, physical, and geopolitical signal in one picture.

283

threat-actor profiles
maintained

1,150+

ransomware victims
tracked in the last 30
days

1,750+

known-exploited
vulnerabilities mapped

80,000+

attack sessions a week
on our own sensors

Figures from Fenestra's own collection, October 2026.

Genuine breadth of collection, backed by analyst expertise — whether your team runs the platform or ours does — is what makes Fenestra intelligence something you can act on.



FENESTRA TI
GLOBAL INTELLIGENCE. CONNECTED INSIGHT.

GET IN TOUCH

LET'S TALK ABOUT WHAT EXPOSURE LOOKS LIKE FOR YOU

Every engagement starts with a conversation about your footprint — your organisation, your people, and the risks that actually apply to you.

contact@fenestra-ti.com

fenestra-ti.com