Navigating The Invisible



Predictive Threat Intelligence in Maritime Operations

About
The Team

- Mehmet Önder Key
- Temel Demir
- Samet Can Taşcı

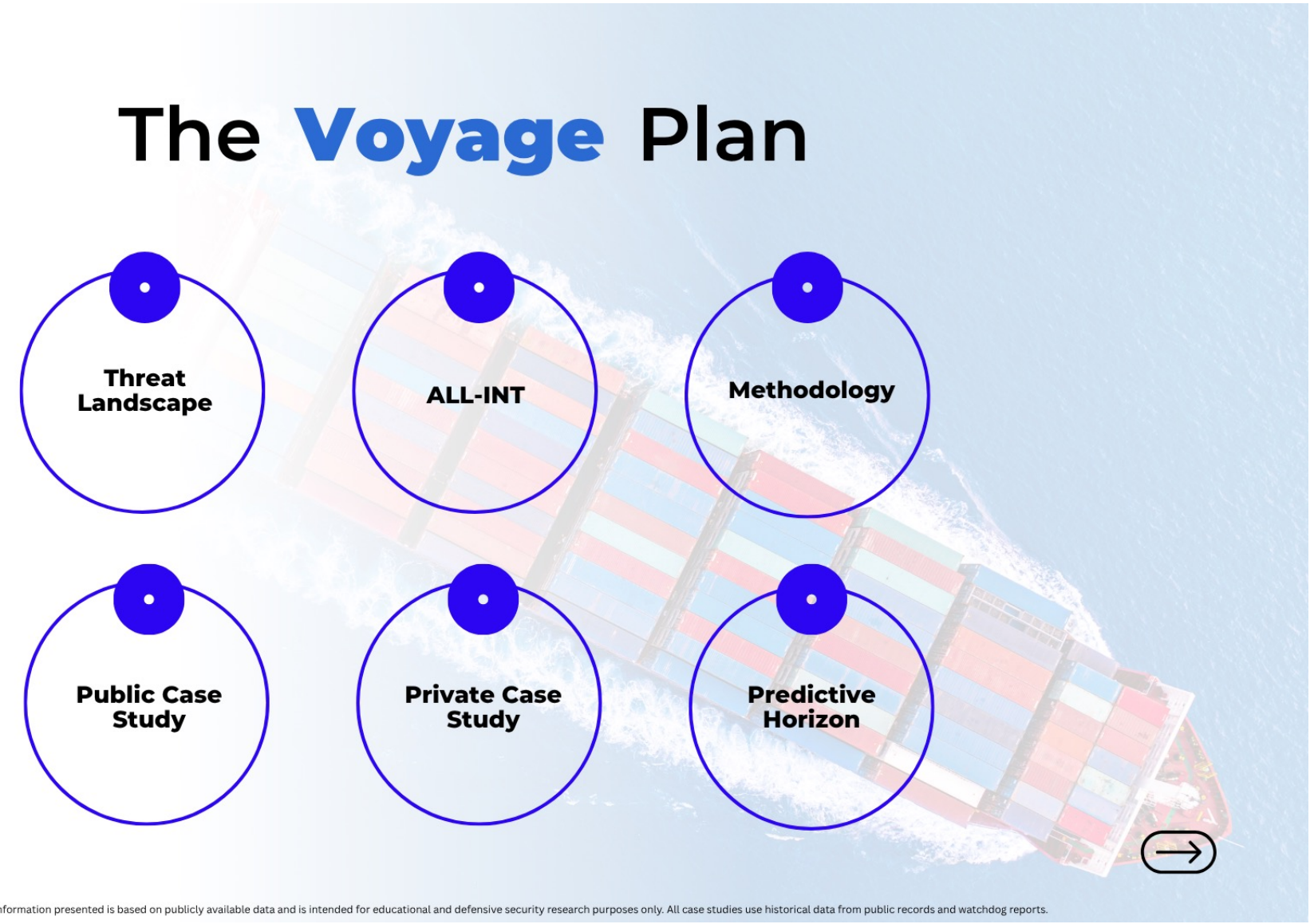


BURKUT

OGRIT
INFORMATION TECHNOLOGIES

RAVENAILABS

The Voyage Plan



Disclaimer: The information presented is based on publicly available data and is intended for educational and defensive security research purposes only. All case studies use historical data from public records and watchdog reports.

Converged Threat Matrix

	PHYSICAL	CYBER
STATE-SPONSORED	Sanctions Evasion, IUU Fishing, Naval Confrontation	Port System Sabotage (e.g., NotPetya on Maersk), GPS Spoofing, Espionage
CRIMINAL	Piracy, Smuggling (Narcotics, Arms), Cargo Theft	Ransomware on shipping lines, Phishing for sensitive data, Business Email Compromise (BEC)
HYBRID (CORE)	Cyber-Enabled Theft: Hacking manifest to locate high-value cargo, then stealing it.	Physical-Enabled Cyber: Gaining physical access to a port or vessel to plant a rogue device.

Basic Osint Arsenal

Vessel Tracking "Where"

- **Source:** AIS (Automatic Identification System). Publicly broadcast VHF data.
- **Tools:** MarineTraffic, VesselFinder, AISHub
- Key Identifiers: IMO (unique lifetime ID), MMSI (radio ID), Call Sign. IMO is king for tracking.

Satellite Imagery "What"

- **Source:** Public & Commercial Satellites.
- **Tools:** Sentinel Hub (EO Browser) for free optical & SAR, Google Earth Pro for historical context.
- **Key Insight:** Verifies what AIS can't see. Did that vessel actually meet another ship?

Corporate & Port Intel "Who"

- **Source:** Maritime databases, company registries, social media.
- **Tools:** Equasis.org (official vessel & company data), LinkedIn (crew/employee profiling), Port Authority websites.

Intelligence Data Spectrum

Data Category	Sub-Type	Description & Use Case	Source Examples (OSINT & Premium)
Vessel Identity & Tracking	AIS (Automatic Identification System)	Real-time & historical vessel position, course, speed. Foundational but fundamentally untrustworthy. 8	MarineTraffic, VesselFinder, Spire, Tradewinds
	Satellite Imagery (SAR/EO)	Visual confirmation of vessel presence, activity (e.g., STS transfers), and spoofing detection. The "ground truth" layer. 10	Sentinel Hub, Maxar, Planet, Starboard
Ownership & Commercial	Corporate Registries & Fleet Data	Identifying Ultimate Beneficial Owners (UBOs), shell companies, and networks to pierce the corporate veil. 10	OpenCorporates, Equasis, Lloyd's List Intelligence
	Chartering & Logistics Data	Understanding commercial activity, cargo details, port calls, and supply chain links. Following the money. 8	Signal Ocean, Maersk/CMA CGM portals
Human Intelligence (HUMINT)	Crew & Personnel Data	Investigating crew members, vessel managers, and their professional networks. Exploiting the human element. 8	LinkedIn, Maritime-Connector, Lloyd's List Profiles
Threat & Risk Intelligence	Security Alerts & Sanctions Lists	Geopolitical risk, piracy warnings, port security status, sanctions updates. Contextualizing vessel behavior. 2	Ambrey, Dryad Global, ICC IMB, OFAC/EU Lists

No single source is sufficient. The craft is in the *fusion* of *data*.

**randomly selected known companies and applications.*

Intelligence Data Spectrum

VECTOR	PLATFORM / TOOL	MISSION	ACCESS	BASIC INFO
Vessel Tracking (AIS)	MarineTraffic, VesselFinder	Real-time tracks, short-term history, vessel details	Freemium	Free tier is limited. Data is self-reported & easily spoofed.
	AISHub	Raw AIS data firehose for bulk analysis	Free (Requires data sharing)	Best for large-scale analysis, but you need the scripting skills to parse the raw data feeds.
	Global Fishing Watch	Fishing activity analysis, vessel identity	Free (API Key)	Hyper-focused on fishing vessels; provides powerful, pre-processed data products.
Satellite Imagery	Sentinel Hub EO Browser	Access Sentinel-1 (SAR) & Sentinel-2 (Optical) imagery	Free	Medium-res, but global coverage & frequent revisits. SAR is your invaluable all-weather, no-blinking eye.
	Google Earth / Earth Engine	High-res historical optical imagery archive	Free	Not real-time. Essential for historical analysis and ground-truthing past events.
	Planet (API/Explorer)	High-frequency, high-resolution imagery on demand	Commercial	Daily global coverage is a game-changer for monitoring specific Areas of Interest (AOIs), but it comes at a high price.
Corporate Records	OpenCorporates	Mapping corporate ownership & shell structures	Freemium	Essential for connecting the dots between shell companies and the people behind them.
	Sanctions Lists (OFAC, EU)	Verifying entities against official watchlists	Free	The definitive ground-truth for compliance and sanctions checks.
Dark Web & Threat Intel	Tor Browser	Accessing .onion sites/forums for chatter & data leaks	Free	The entry point to the dark web. Extreme Operational Security (OPSEC) is not optional.
	Threat Intel Platforms	Automated monitoring of forums, paste sites, and markets	Commercial	Scans for keywords, leaked credentials, and actor chatter related to maritime targets. Automates the hunt.

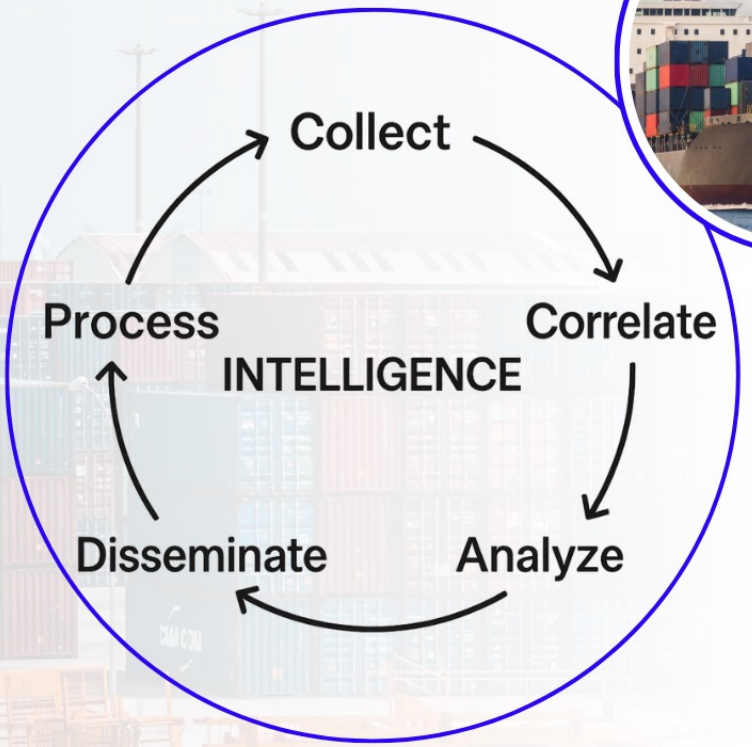
No single source is sufficient. The craft is in the *fusion* of *data.*

randomly selected known companies and applications. The **private case study will include different sources and specific applications.*

Methodology

Intelligence Cycle

- **1. Collect:** Gather raw data from our arsenal (AIS tracks, SAT imagery, corporate records).
- **2. Process:** Structure the data. Filter out noise. Translate raw AIS positions into a coherent track on a map.
- **3. Correlate:** This is the critical step. Fuse different data types. Overlay the AIS track on a satellite image. Match a vessel's IMO number to its corporate owner.
- **4. Analyze:** Develop insights. Identify anomalies and patterns. Form a hypothesis. Why did this ship turn off its AIS here? Is this meeting suspicious?
- **5.Disseminate:** Create an actionable intelligence product. (Like the case studies we're about to see).





Unmasking the Ghost Tanker



Public Case Study

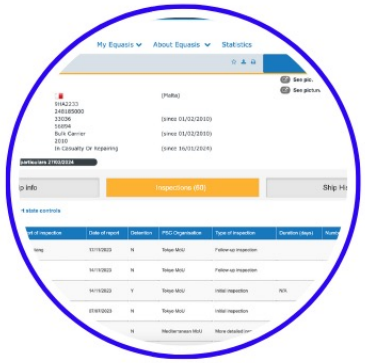
Objective
To prove a tanker suspected of loading sanctioned oil is engaged in illicit activity.

Methodology
The five-step intelligence cycle (Collect, Process, Correlate, Analyze, Disseminate)

Target
"MV Sea Serpent" (Broadcast Name), IMO: 9178655 (Spoofed Identity)
**fake imo number*



First Signals



Step 1: COLLECT

AIS Data: Real-time and historical track data for "MV Sea Serpent" (IMO: 9178655) is gathered from MarineTraffic.

Corporate Data: Official vessel records associated with the IMO number are queried via Equasis.org.



Step 2: PROCESS

The AIS track is mapped. The vessel's declared destination is listed as "Singapore."

However, its actual heading is towards the west of the Strait of Malacca, a known illicit STS (Ship-to-Ship) transfer zone. This is the first behavioral anomaly.



Step 3: CORRELATE

CRITICAL FINDING 1: "ZOMBIE VESSEL"

The Equasis query reveals IMO 9178655 actually belongs to a vessel named "Oceanic Pride."

Official status: "Broken Up" (Scrapped). Date: 2023.

Conclusion: The vessel is using a stolen identity from a scrapped ship. We are tracking a ghost.

CRITICAL FINDING 2: "GOING DARK"

The vessel intentionally disables its AIS transponder upon entering the illicit transfer zone. The signal vanishes.



CORRELATE

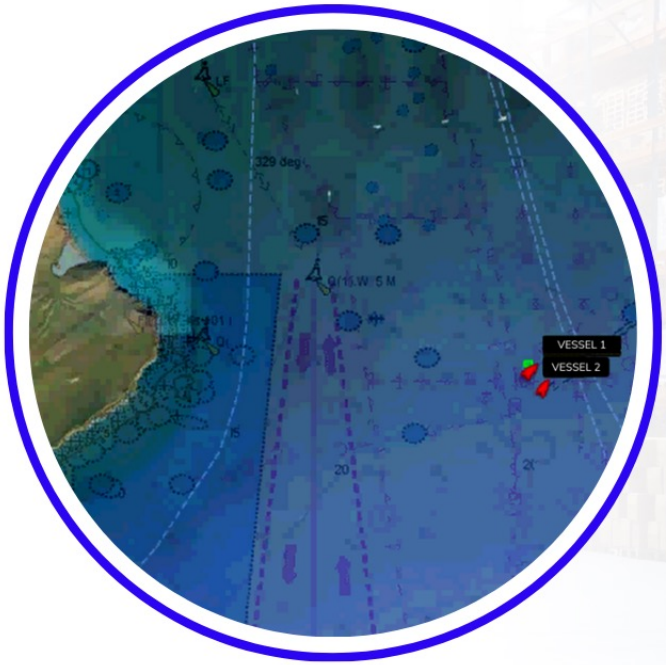
>>

Vector: Sentinel-1 (SAR) satellite imagery archives are tasked for the time and coordinates of the AIS outage.
Technical Advantage: SAR (Synthetic Aperture Radar) provides clear imagery regardless of clouds, fog, or darkness.

Finding: The SAR image physically confirms the presence of two large tankers side-by-side (in an STS transfer configuration) at the specified location.

Conclusion: The AIS blackout was a deliberate act to conceal an illicit transfer. Digital suspicion is now proven with physical evidence.

Last Signals



Step 4: ANALYZE

Hypothesis: An unidentified tanker is illegally using the identity of a scrapped vessel to conduct a sanctioned STS transfer and load illicit cargo. The vessel is now fully laden and likely heading east.

Step 5: DISSEMINATE

Product: An actionable intelligence report is created for relevant authorities.

Summary: "Zombie Vessel" identification and illicit STS transfer summary.

Evidence: AIS track, corporate record discrepancy, and the SAR image.

Recommendation: Flag the vessel as HIGH RISK for immediate tracking and inspection at its next port of call.

Predictive Horizon

```
    score += vessel["ais_gaps_detected"] * WEIGHT_AIS_GAP

    # 2. Score for High-Risk Zone
    if vessel["current_location"] in HIGH_RISK_ZONES:
        score += WEIGHT_RISK_ZONE

    # 3. Score for ID Spoofing
    if vessel["official_name"] != vessel["broadcast_name"]:
        score += WEIGHT_ID_SPOOFING

    return score

def analyze_fleet_risk(vessels):
    """
    Analyzes a fleet of vessels, calculates their risk scores,
    and returns a sorted list of results.
    """
    analysis_results = []
    for vessel in vessels:
        score = calculate_risk_score(vessel)
        analysis_results.append({
            "name": vessel["broadcast_name"],
            "imo": vessel["imo_number"],
            "score": score,
            "risk_level": "High" if score >= RISK_THRESHOLD else "Medium" if score > 0 else "Low"
        })

    # Sort results from highest score to lowest
    sorted_results = sorted(analysis_results, key=lambda x: x['score'], reverse=True)

    return sorted_results

# --- MAIN EXECUTION AND OUTPUT ---
if __name__ == "__main__":
    fleet_analysis = analyze_fleet_risk(mock_vessels_data)

    print("="*60)
    print("== GLOBAL SUPPLY CHAIN PROACTIVE RISK ANALYSIS DASHBOARD ==")
    print("="*60)
    print(f"{'VESSEL NAME':<20} {'IMO':<15} {'RISK SCORE':<15} {'STATUS'}")
    print("-"*60)

    for item in fleet_analysis:
        status_flag = "🚨 ALERT: HIGH RISK! 🚨" if item['risk_level'] == "High" else ""
        print(f"{item['name']:<20} {item['imo']:<15} {item['score']:<15} {status_flag}")
```

```
============================================================
== GLOBAL SUPPLY CHAIN PROACTIVE RISK ANALYSIS DASHBOARD ==
============================================================
VESSEL NAME          IMO             RISK SCORE      STATUS
------------------------------------------------------------
The Ghost            UNKNOWN         90              🚨 ALERT: HIGH RISK! 🚨
Evergreen            8918236         80              🚨 ALERT: HIGH RISK! 🚨
Gulf Prospector      9780597         50
Atlantic Trader      9237694         20
MV Serenity          9419341         0
```

*based on this logic a simple python script with sample data and output

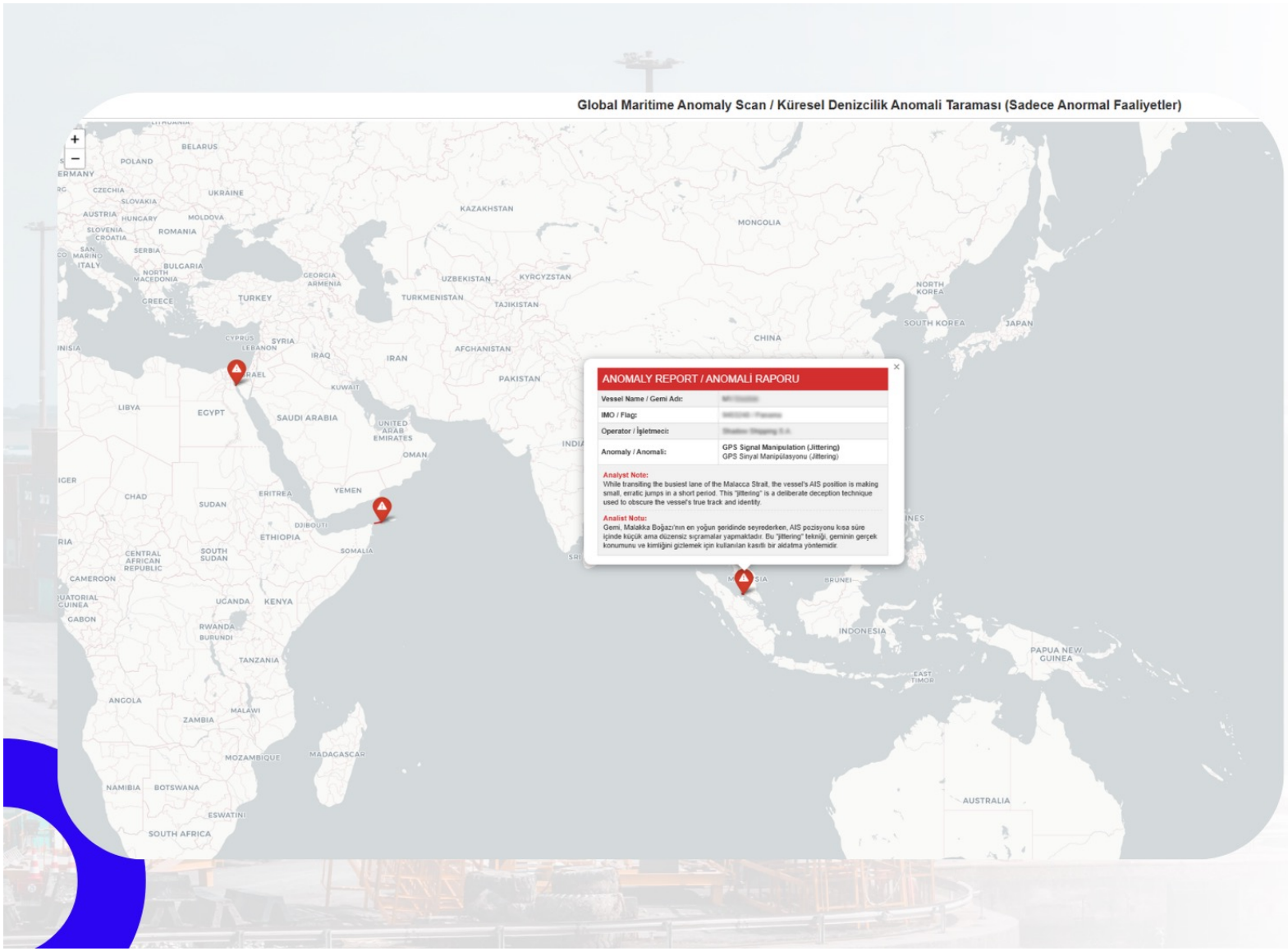
AIS Gaps: A lost AIS signal may indicate an intentional attempt to remain “dark,” but it could also be due to technical issues or weak satellite coverage. Therefore, it is assigned a moderate weight.

Navigating in a High-Risk Area: aimlessly navigating in an area known for piracy (e.g., the Gulf of Guinea) or near a sanctioned port is highly suspicious. This behavior is assigned a high weight.

Identity Fraud: A mismatch between the published ship name and the official name in the IMO registry is a clear and deliberate act of deception. This is a significant danger signal and should be assigned the highest weight.

The goal is not to predict the future, but to prevent threats through anomaly detection and risk scoring. This is possible through automation and behavioral analytics. A simple but effective risk scoring model can be built as follows

(RiskScore = (w1 × AIS_Gaps) + (w2 × Loitering_in_RiskZone) + (w3 × ID_Spoofing))



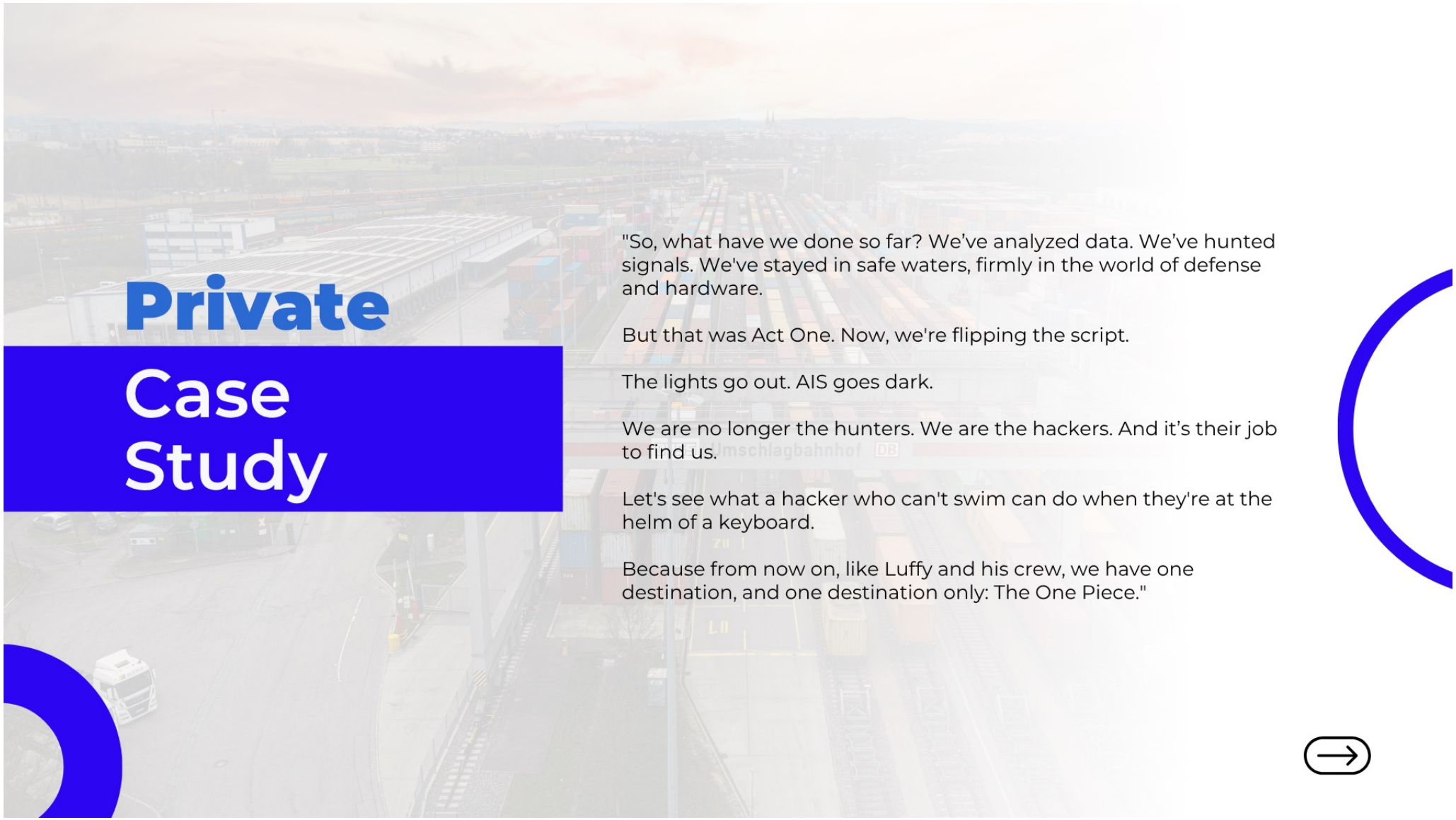
Global Action Horizon

More data...
More information...
More correlations...
More risk scoring...
More algorithms...
More insights...
More dashboards...
And finally.
More “MORE!”
MaritimeOperationsRiskEngine

Shedding Light ON Maritime WITH Data



Private Case Study & Real Life & Educational Only



Private Case Study

"So, what have we done so far? We've analyzed data. We've hunted signals. We've stayed in safe waters, firmly in the world of defense and hardware.

But that was Act One. Now, we're flipping the script.

The lights go out. AIS goes dark.

We are no longer the hunters. We are the hackers. And it's their job to find us.

Let's see what a hacker who can't swim can do when they're at the helm of a keyboard.

Because from now on, like Luffy and his crew, we have one destination, and one destination only: The One Piece."

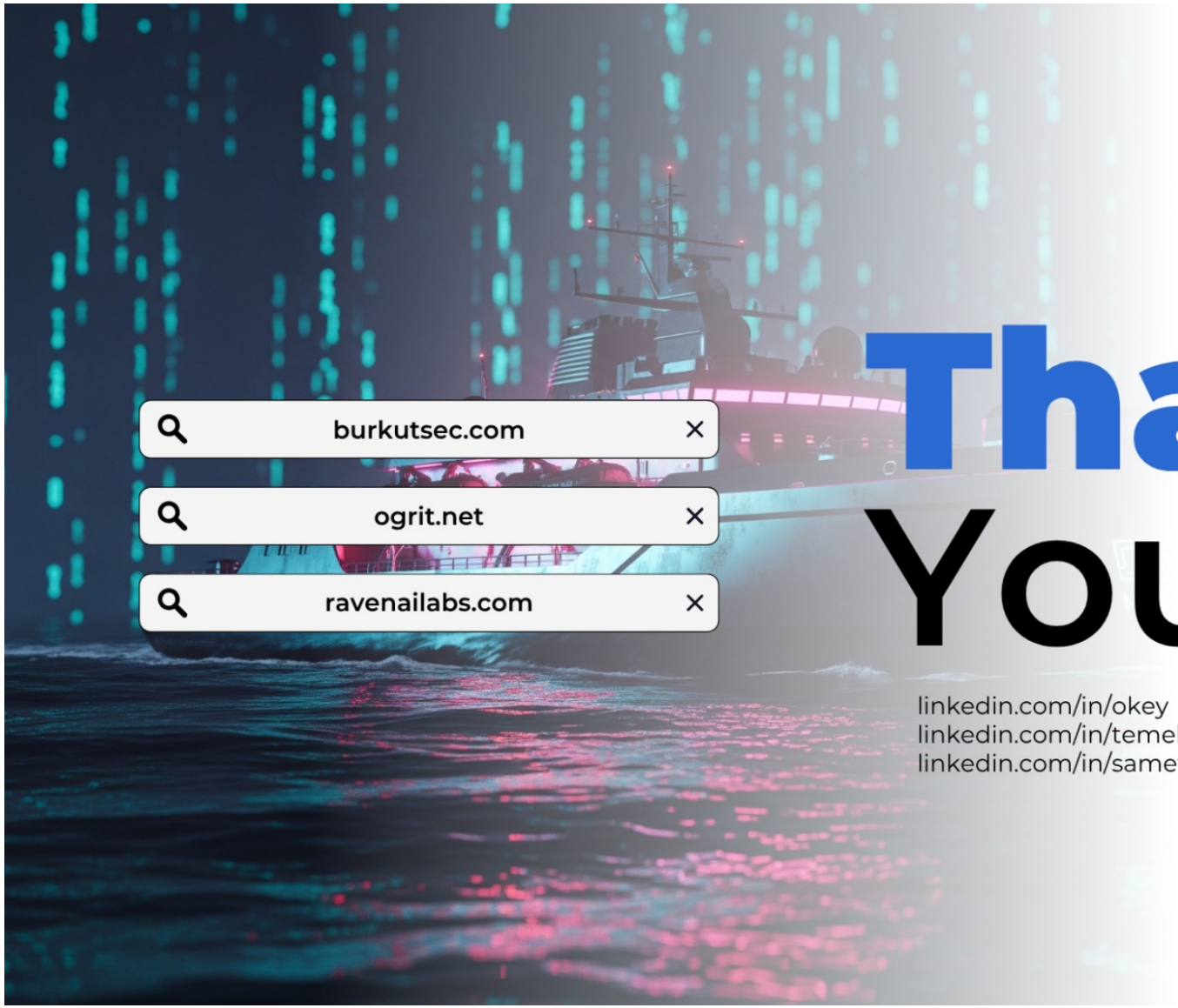


Live Demo

"Quick heads-up for this next section:

No photos, no videos, please.

I've already redacted or blurred all the sensitive stuff to avoid legal trouble, so let's keep it that way." :)



Thank You!

linkedin.com/in/okey
linkedin.com/in/temel-demir
linkedin.com/in/sametcantasci