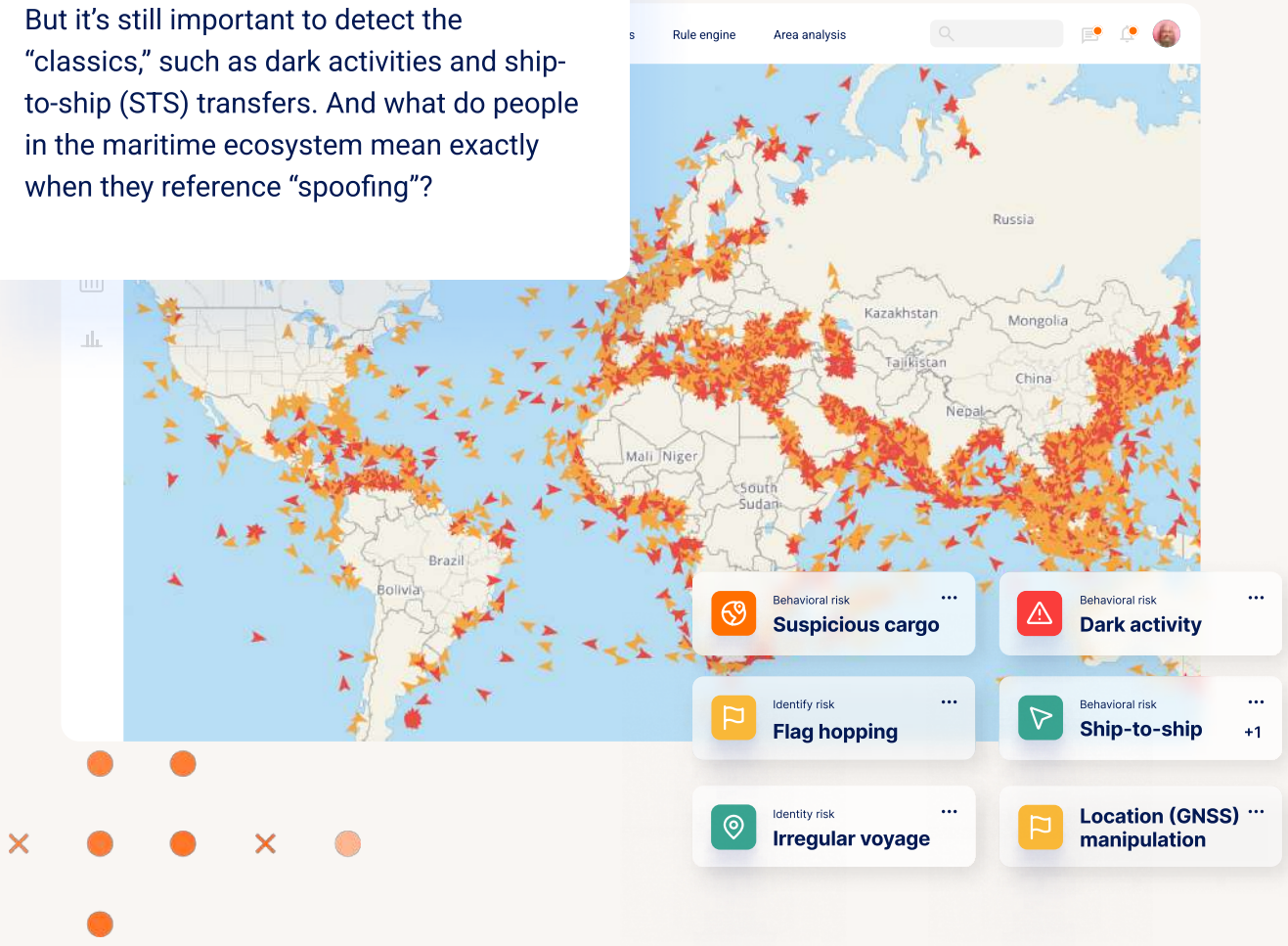
WINDWARD

DSPs guide

From Dark to Zombie: the Full Deceptive Shipping Practices Guide

Zombie Vessels? AIS handshakes? Deceptive shipping practices (DSPs) have become complicated, sophisticated, and nearly unrecognizable in recent years. But it's still important to detect the "classics," such as dark activities and ship-to-ship (STS) transfers. And what do people in the maritime ecosystem mean exactly when they reference "spoofing"?



What You'll Find in the Guide

Our comprehensive guide to deceptive shipping practices details all deceptive shipping practices from the classic one to the newest, plus a brief historical overview to ensure complete coverage of this important subject matter. We will also look at how the Russia-Ukraine conflict has impacted and changed DSPs in recent years.

Deceptive actors are quick to adapt their tactics and exploit the vulnerabilities inherent in legacy systems, plus new vulnerabilities as they emerge. They constantly seek loopholes in existing regulations and sanctions, and leverage advancements in communication, logistics, and data manipulation, to try to stay ahead. This makes it difficult for businesses, regulatory bodies, and law enforcement agencies to develop and implement effective preventive measures in a timely manner.

Another factor: geopolitical conflicts often have massive impact on the maritime ecosystem and Russia's invasion of Ukraine triggered a whole new round of sanctions that left organizations struggling to quickly comply. But there will always be a new conflict (unfortunately), or technological innovation someone will try to exploit.

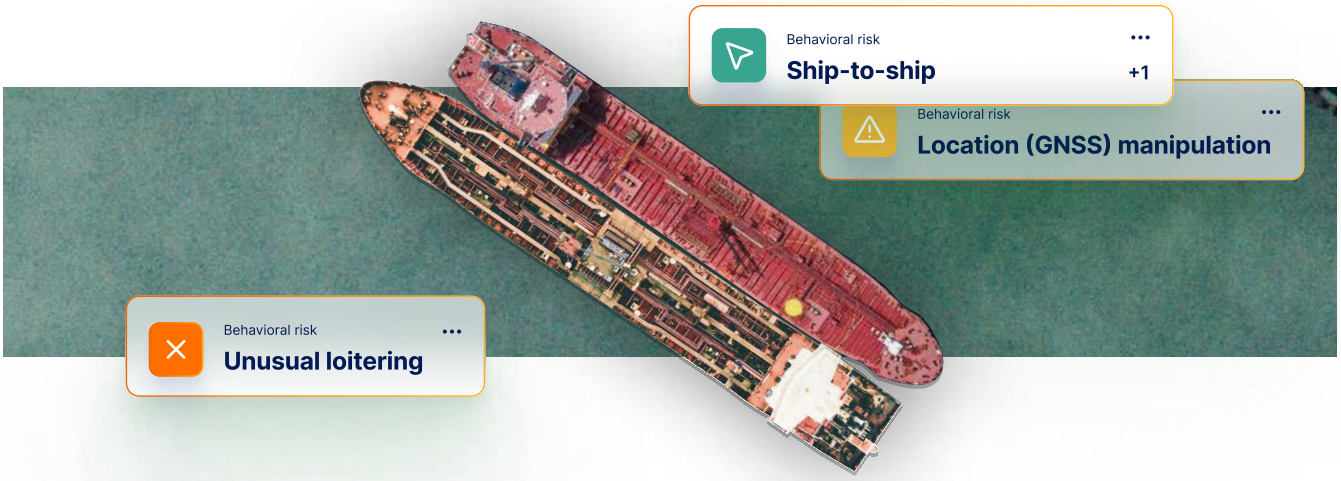
This guide aims to provide you with an in-depth understanding of the evolving nature of DSPs. We will start with the release of the OFAC guidelines in 2020, and then highlight more recent tactics Windward has identified via our Maritime AI™ platform.

By staying informed about the evolving nature of these practices, you can navigate the complex shipping landscape with confidence and protect yourself from falling victim to deceptive schemes.

Defining DSPs and the Intended Audience

Deceptive shipping practices (DSPs) are tactics utilized by bad actors to evade detection, sanctions, and regulations while engaging in illegal operations, such as oil smuggling and illegal trading. These practices can make it difficult to track the movement of cargo, identify the true owners of vessels, and enforce sanctions.

New tactics have emerged, making identity changes look as quaint as a 17th century tactic. An umbrella term called “spoofing” has been driving the maritime industry crazy with multiple interpretations. Within this concept, there are multiple tactics involving the use of various identities, transmitters, and even location (GNSS) manipulation methodologies that are growing at an exponential speed compared to previous deceptive shipping practices.



This guide provides an overview of deceptive shipping practices, including:

- Types of deceptive shipping practices
- Red flags that may indicate deceptive shipping practices
- Steps you can take to mitigate your risk of exposure to deceptive shipping practices

The guide is intended for anyone who is involved in the maritime industry, including:

- Shipping companies
- Traders
- Insurance companies
- Banks
- Government & defense agencies
- Intelligence agencies
- Freight forwarders
- Importers & exporters
- Beneficial cargo owners (BCOs)

The Shift in 2020

An advisory published in May 2020 by U.S. authorities, including the Department of the Treasury's Office of Foreign Assets Control (OFAC), Department of State and the Coast Guard, listed seven key DSP tactics commonly used by sanctions evaders to disguise illicit trade.

This was the first time U.S. authorities detailed the responsibilities and expectations that private businesses connected to the maritime sector must adhere to. Beyond merely mapping these practices, the advisory laid out recommendations for each industry on how to proactively conduct due diligence that can identify these practices, "in order to limit the risk of involvement with sanctionable or illicit activity."

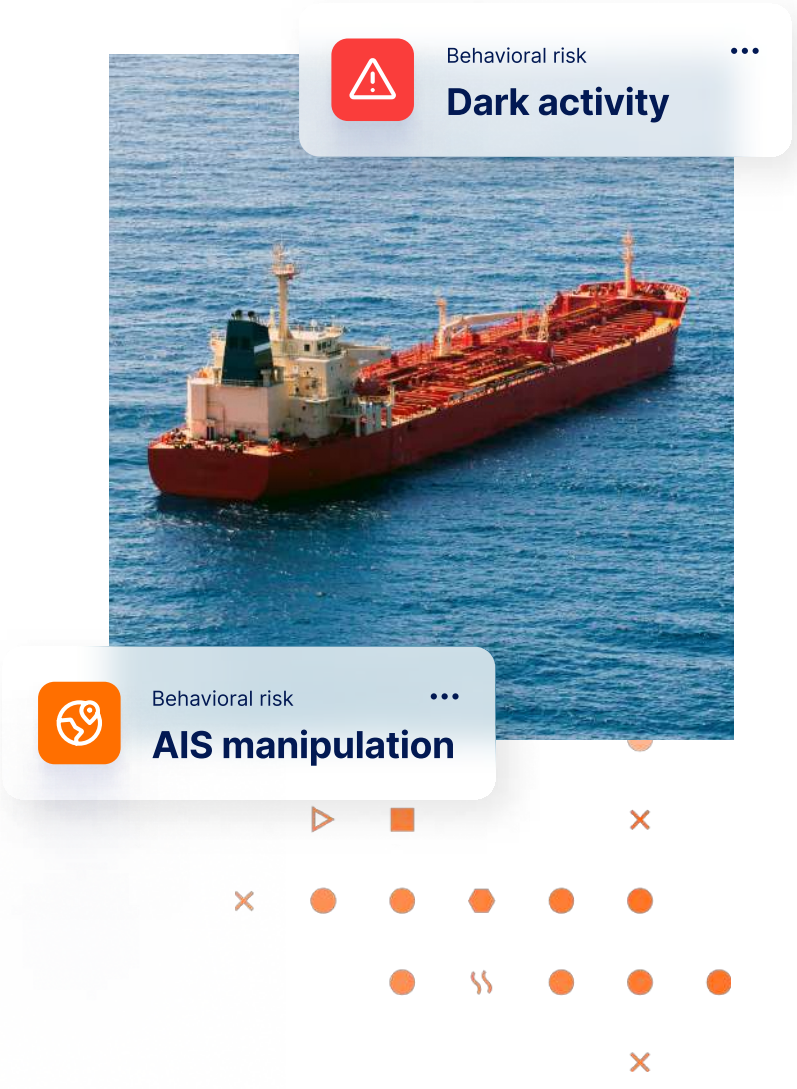
OFAC's Impact

Why was this OFAC advisory such a seismic shift?

Previously, traditional sanctions screening best practices were built on "list matching": every customer or transaction was screened against lists of designated people, organizations, and entities to identify blocked parties. This practice had its challenges around efficiency and accuracy, but in essence, it compared data with data to raise red flags on those already designated by sanctioning bodies. It didn't deal with suspicions or gray areas, and had no predictive capabilities to stay ahead of the cat-and-mouse game.

The 2020 advisory was an acknowledgment that mere list screening for sanctions violators/illicit actors was too little, too late. AIS was widely depended upon to understand trading patterns during that period and it offered useful information, but raw blips are not enough in today's era. Accurately detecting deceptive practices, such as AIS manipulation, ship-to-ship transfers, or voyage irregularities requires insights and predictive analytics. This type of input can only be created through a thorough investigation, applying domain expertise and context to the data to make sense of it and manage your risk.

Second, identifying DSPs often highlights potential sanctions evaders to avoid. The goal: identifying vessels and types of vessels that are at risk of designation, regardless of whether they are on a list or not. While list matching can be efficiently automated, every shipping-related transaction today needs to be analyzed individually by a domain expert before making a decision, making it costly and time-consuming. Let's take a look at the seven DSPs identified by OFAC, as well as some of the newer ones.



3 Types of Deceptive Shipping Practices

Before discussing the evolution of deceptive shipping practices, it is important to quickly define terms to ensure there is a standardized conceptual framework. The industry tends to group many different activities as “spoofing,” which is too general and leads to confusion.

To truly and accurately identify and mitigate these risks, we must first define them to understand exactly what we are looking for and how it’s done.

We can conceptually group DSPs into three categories

The Classics
the techniques from the OFAC advisory

Identity Games
newer deceptive practices that we are seeing more frequently

Seafloor Strategies
cutting-edge techniques

The Classics

These are the 7 DSPs identified by OFAC

Disabling or manipulating the AIS – vessels engaged in illicit activities sometimes intentionally disabled AIS transponders or manipulated data transmitted to mask movements.

Voyage irregularities – bad actors attempt to disguise the ultimate destination or origin of cargo by using indirect routing, unscheduled detours, or transit or transshipment of cargo through third countries.

Physically altering vessel identification – vessels involved in illicit activities often painted over vessel names and IMO numbers to obscure their identities and pass themselves off as different vessels.

False flags and flag hopping – illicit actors falsified the flag of their vessels to mask illicit trade. They also repeatedly registered with new flag states to avoid detection, also known as “flag hopping.”

Falsifying cargo and vessel documents – sanctions evaders falsified shipping documentation, primarily pertaining to petroleum, petrochemicals, petroleum products, metals, or sand to disguise their origin.

Complex ownership or management – evaders used shell companies and/or multiple levels of ownership and management, to disguise the ultimate beneficial owner of cargo or commodities.

Ship-to-ship (STS) transfers – STS transfers at sea, especially at night or in high-risk areas for sanctions evasion or other illicit activity, are frequently used to evade sanctions by concealing the origin or destination of cargo.

Identity Games

"Going dark" (disabling the AIS system) is still popular, but sophisticated bad actors now understand that a vessel worth millions of dollars is too expensive to risk going dark for a single transaction.

If identified, the vessel, crew, and owners will not only be exposed to sanctions, but will also suffer from seized cargo and lasting reputational damage. And having a vessel idle for a long period of time could prove costly.

Instead of trying to conceal vessel behavior, many bad actors have changed direction. They now seek to reap the benefit of illegal activities while projecting a veil of "business as usual." In other words, they are "hiding in plain sight."

Dual transmission
the use of multiple AIS transmitters onboard a single vessel transmitting different entities with separate International Maritime Organization (IMO) numbers.

Identity theft
when one vessel assumes the identity of another operating vessel, creating a duplication of the same transmitted identifiers.

Flag hopping
repeatedly changing transmitted MMSIs (flags) to avoid detection. This practice is also used as a legitimate financial tactic, making it difficult to label as an illicit activity.

Identity laundering
when one or more ships deliberately tamper with or misrepresent aspects of their physical, digital, and registered identities. This is done to obfuscate the original identity and necessitates at least one ship assuming a fraudulently obtained, IMO-registered "shell" identity.

In a type 1, or "direct" laundering operation, the "dirty" vessel directly assumes the shell identity. In a type 2, or "indirect" operation, a "clean" vessel assumes the shell identity and the dirty vessel assumes the clean vessel's now-vacant identity (from C4ADS {2021}. Unmasked – Vessel Identity Laundering)

Identity tampering
the deliberate falsification of a vessel's broadcasted data on AIS and/or alterations to its physical features, to misrepresent its identity (from C4ADS (2021). Unmasked – Vessel Identity Laundering)

** "dirty" in this context refers to a vessel subject to public derogatory reporting, or law enforcement action that may inhibit its ability to engage in commercial operations at will. "Clean" refers to a vessel that has not been the subject of derogatory reporting or law enforcement action that would inhibit its ability to engage in normal commercial activity. So-called "dirty" vessels may masquerade as clean vessels to conduct activities that would be prohibited or difficult under their own identities. (from C4ADS {2021}. Unmasked – Vessel Identity Laundering)*

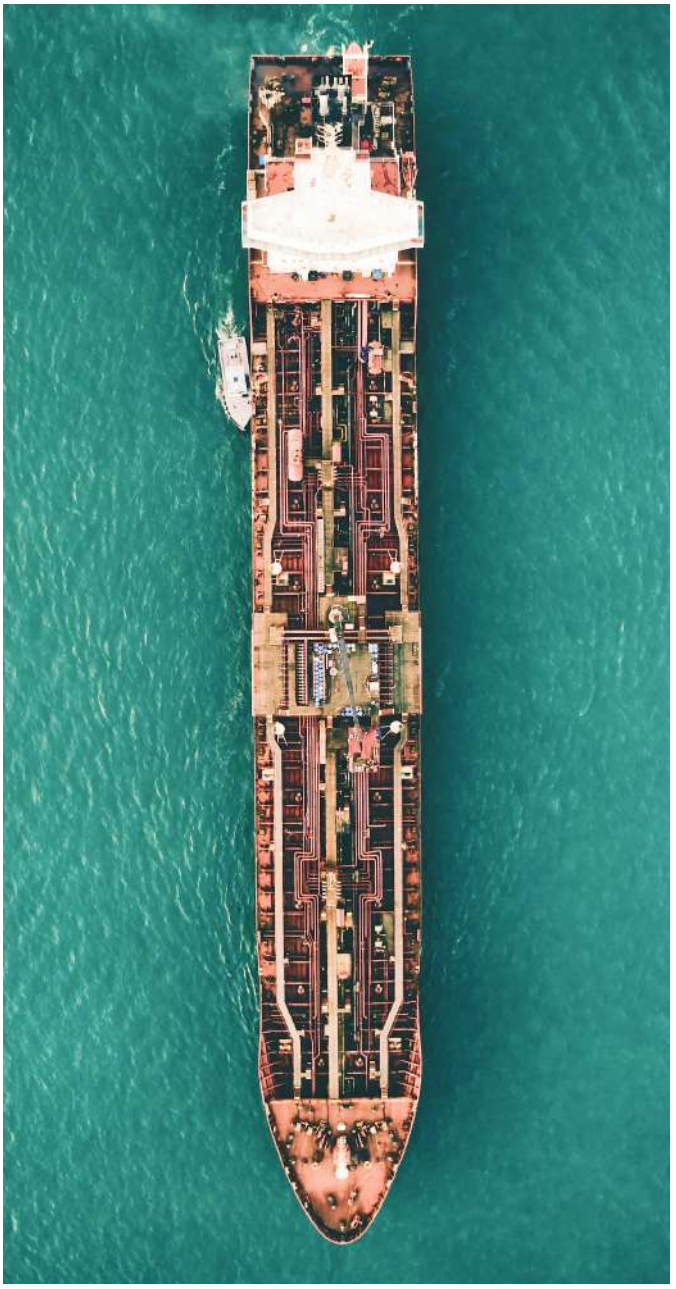
Seafloor Strategies

Creatures that hide on the seafloor have mastered the art of hiding from predators, despite being in plain sight. “Seafloor Strategies” describes the latest, most advanced camouflage tactics discovered by Windward’s Maritime AI™ technology and experienced experts.

Location (GNSS) manipulation
the use of a machine-generated location/path to disguise the true location of the vessel. Multiple methods have been identified to carry out this deception, including false transmission onboard the vessel and third-party onshore accomplices. Windward has a patent-pending GNSS model.

Zombie vessel
the use of a scrapped vessel’s identity to perform illicit operations without legal repercussions.

AIS handshake
the use of a decoy vessel as a disguise. The dirty vessel will assume the clean vessel’s identity as they are sailing at close proximity, while the clean vessel makes its way to its destination while dark. Upon returning, the vessels will recreate the switch, leaving the clean vessel unscathed.



The Tremendous Impact of Russia's War

Hardly anyone expected a full-scale invasion of Ukraine on February 24, 2022. Once the shock wore off, most experts seemed to think the conflict would end quickly.

With the West's economic vice continually tightening on Russia, there has been an increase in deceptive shipping practices, particularly a combination of dark activities, location (GNSS) manipulation, and ship-to-ship meetings. New hubs have continued to pop-up for concealing illicit activities as old ones draw increased scrutiny, and Iran and Russia strengthened their trade routes.

The challenge involving many different types of cargo, so unprepared organizations are now dealing with the same issues faced by oil companies following OFAC's 2020 pronouncement. This has been a particular challenge for the dry cargo industry, which previously has not had to focus on potential sanctions violations. They do not have the necessary work processes in place, and it is expensive to build one and difficult to create the required flows without the requisite experience/expertise.

Additionally, as detailed in our report, Illuminating Russia's Shadow Fleet, Russia's war against Ukraine created a "shadow fleet" to smuggle oil in an attempt to evade sanctions.

Three-Tiered System

Windward's Maritime AI™ platform identified a three-tiered system of vessels to paint an accurate picture of Russian oil smuggling:

Cleared fleet – tankers not exhibiting any suspicious conduct, such as flag hopping or irregular ownership structure. It is important to be able to quickly identify these vessels, so that maritime organizations are not paralyzed by false positives and indecision that will further hamper global trade.

Gray fleet – a completely new phenomenon evolving from the Russia war. Overseas companies have been quickly established following the outbreak of the war, to obscure vessel origins and ownership, and to appear law-abiding/non-sanctioned. This fleet is described as "gray" because it is difficult to determine legality and sanctions compliance in many cases. A significant number of these vessels also switch flags ("flag hopping") frequently.

Dark fleet – this fleet often utilizes "dark activities" (the intentional disabling of the automatic identification system) to move wet cargo, along with other deceptive shipping practices (DSPs), such as ID and location (GNSS) manipulation.

Staying Ahead of the Cat and Mouse Game

DSPs are evolving faster than ever, due to the advanced and cheap technology that is readily available to bad actors. These new tactics allow illicit actors to essentially hide in plain sight and achieve their objectives, without risking their crew or vessel's reputation.

It has become understood in the maritime domain that turning off the AIS transmitter is an immediate red flag detectable by nearly every maritime domain awareness system in the market. At first glance, it seems like dark activity is keeping a steady growth rate, unless data is positioned in the right sanctions context.

It's also important to note that trying to detect dark activity without the proper maritime detection technology will lead to endless false positives that will waste your resources (financial and human).

By combining vessels'/crews' intent, domain expertise, and Maritime AI™ technology, Windward can quickly flag the activities that are worth investigating. Our dark activity insights capability goes beyond static data to accurately differentiation of dark activity from "lost and found"/legitimate transmission gaps.

Windward also provides AI-based predictions from our patent-pending model on the vessel's like destination, while the vessel is dark.

Mitigate the Damage

Bad actors will not stop trying to innovate during this game of cat and mouse, because the potential rewards of illegal activities, such as crude oil smuggling, are obviously high. Without the right technology, legitimate shipping stakeholders (coast guards, government agencies, shipowners, traders, beneficial cargo owners, and freight forwarders, etc.) don't stand a chance.

As mentioned, Russia's war has intensified DSPs and unfortunately, history shows there will always be another geopolitical conflict that triggers sanctions. With criminal networks hiding in plain sight, now is the time to invest in a spotlight.

Until now, it has been commonly believed that:

- **Non-transmitting vessels = bad actors**
- **Transmitting vessels = safe ships to**
- **work with**

But things are a lot more complicated than they seem. It's nowhere near as simple as merely screening for sanctions lists, or detecting dark activity – although that is still relevant and necessary. The cat-and-mouse game continues to evolve at warp speed, with ships being seemingly resurrected from the dead and complicated ID location manipulation schemes.

To find and expose the hiders, and mitigate the damage they can cause, government agencies, traders, shipowners, and coast guards will need to quickly understand circumstances and contexts, via maritime expertise and an innovative artificial intelligence system that can automatically flag illicit activities and quickly determine what is actionable.

Watch Windward Expose the Hiders

To the demo page