HIVESTØRM

STORM PLATFORM

MARITIME & LOGISTICS / SECTOR

PRODUCT DATASHEET

CRITICAL SUPPLY-CHAIN INFRASTRUCTURE · SHIP TO SHORE · REAL-TIME CONTAINMENT · SOVEREIGN BY DEFAULT

THE PROBLEM

Maritime and logistics move the world's goods, and the supply chains they run are critical national infrastructure under sustained attack. A single ransomware outbreak has already shut down a global shipping line and the ports it touched — costing hundreds of millions and stalling supply chains for weeks.

The estate spans vessels at sea and the logistics chain ashore: shipboard navigation, propulsion and cargo systems act at machine speed on intermittently-connected networks, while terminal operating systems, cranes, and freight and warehouse automation run the flow on land. A compromise can misroute a vessel, falsify a cargo manifest, or take a terminal offline.

Navigation and positioning signals can be spoofed or jammed, cargo and routing systems tampered with, and much of the shipboard and terminal estate is long-lived equipment that can't simply be patched or re-architected.

And manifest, routing and customs data harvested today can be decrypted once quantum computing matures, so the data crossing your networks now has a shelf life measured in decades.

THE SOLUTION

HiveStørm puts one engine across the shore-side logistics IT estate and the OT from vessel to terminal. It learns the normal rhythm of voyages, cargo flows and terminal operations, surfaces only what is genuinely new, and contains the threat autonomously at machine speed — before a vessel is misrouted, a manifest is falsified, or a terminal goes down. It runs sovereign and keeps protecting a vessel even when its satellite link drops.

It deploys air-gapped and on-premise by default, protects every link with post-quantum cryptography, and seals every action into a tamper-evident, audit-ready record under sovereign custody.

> *One engine, ship to shore — sovereign, real-time, provable.*

01 KEY BENEFITS

- Defend the supply chain against nation-state adversaries.
- One engine across vessels, terminals and the logistics chain.
- Threats contained in seconds — before a vessel, manifest or terminal is hit.
- Understands the sequence, not just the alert.
- Your routing and cargo data never leaves your control.
- Tamper-evident, audit-ready records for regulators and insurers.

02 FEATURE SPOTLIGHT

Protects the vessel at sea

Runs sovereign on board, and keeps protecting navigation and cargo systems even when the satellite link drops.

Sees the whole attack, not just the alarm

Maps which vessels, terminals or systems a compromise can reach, so you contain the right thing.

Learns the rhythm of the chain

Flags the command or instruction that doesn't belong, even when no signature has ever seen it.

Quantum-safe from day one

Protects manifest, routing and customs data against "harvest now, decrypt later" — without a multi-year migration.

DEPLOYMENT

Air-gapped and on-premise by default — real-time defence from the bridge to the terminal, afloat or ashore.

COMPLIANCE & ASSURANCE

Built on NIST-standardised post-quantum cryptography, with tamper-evident, audit-ready records. Sovereign and on-premise by default.

WHAT IT IS

Two defences fused into one sovereign platform.

HiveStørm is a **Sovereign XDR** that detects and contains the threat, and a **post-quantum cryptographic layer** that protects your data as it moves. One platform does both — across the vessel, the terminal and the logistics chain ashore. Both run on one stateful event intelligence engine — it remembers what came before, so it sees patterns, not isolated events.

PILLAR A

SOVEREIGN XDR

DETECT & CONTAIN

- Watches every signal across your shore-side IT and your maritime OT — bridge systems, cargo and propulsion, terminal operations and freight automation — learns what normal looks like, and contains what doesn't belong autonomously, at machine speed, before a vessel, manifest or terminal is hit.
- **Sovereign** means it runs entirely inside your estate, in your jurisdiction, on your hardware — nothing leaves, nothing depends on a foreign service — and it keeps working when a vessel's link drops.
- Extended detection and response that acts in seconds — without an analyst sat in the loop waiting to investigate.

PILLAR B

POST-QUANTUM DEFENCE

PROTECT DATA IN TRANSIT

- Every link — between vessels, terminals, freight systems and head office — is encrypted with post-quantum key exchange, so traffic harvested today can't be decrypted later ("harvest now, decrypt later").
- Protects legacy shipboard and terminal OT in place: a drop-in post-quantum layer sits in front of equipment that can't speak modern cryptography, with no re-engineering [confirm].
- Quantum-safe from day one — not waiting on a multi-year migration across fleet and shore.

ONE LOOP, NOT TWO PRODUCTS DETECT ⇄ RE-KEY

Detection and cryptography aren't two bolted-together products — they work as one loop. When the XDR layer detects a compromise indicator anywhere in the estate, it triggers the cryptographic layer to re-key the affected channels in seconds. The defence moves with the adversary, not against a calendar.

> *Most vendors sell you threat detection or post-quantum cryptography. HiveStørm fuses them.*

04 WHAT THIS MEANS FOR THE OPERATOR

- **Detection and encryption defend the supply chain as one system, not two tools.**
- **Your routing, manifest and customs data stays private — today and against tomorrow's quantum threat.**
- **Legacy shipboard and terminal systems get quantum-safe protection without being ripped out or rebuilt.**
- **A single sovereign platform that keeps protecting a vessel even when its link drops.**

UNDER THE HOOD

A stateful event intelligence engine ingests from any source and keeps the memory of what came before. Built on NIST-standardised post-quantum algorithms (`ML-KEM`, `ML-DSA`) with zero foreign dependencies — sovereign, and standards-based.

05 NEXT STEP

STEP 01
DEMO
Guided Storm Platform demonstration

→

STEP 02
EXPOSURE REPORT
Storm Rune cryptographic exposure report

→

STEP 03
BOUNDED POC
Scoped proof-of-concept, your environment