HIVESTØRM

STORM PLATFORM

INDUSTRIAL & ROBOTICS / SECTOR

PRODUCT DATASHEET

ONE ENGINE · IT + OT · REAL-TIME CONTAINMENT · SOVEREIGN BY DEFAULT

THE PROBLEM

Operational technology now sits on routable networks it was never designed to defend. The air gap that once protected the plant is gone — IT and OT have converged, and ransomware groups know it.

Production lines, robots and the control systems beneath them act at machine speed, in the exact gap where a human operator can no longer keep up with the decision. A single compromise can halt a line, threaten safety, or take critical national infrastructure offline.

The equipment at risk is often legacy kit that cannot simply be patched or re-architected — even as regulators demand that the defence be real-time, sovereign, and provable after the fact.

THE SOLUTION

HiveStørm puts a single engine across both your IT and your OT estate. It learns the normal rhythm of your operation, recognises routine activity, and surfaces only what is genuinely new — then contains the threat autonomously, at machine speed, before it can reach the line.

It deploys on-premise and sovereign by default, so nothing leaves your estate. It protects legacy OT in place, without a costly re-engineering programme. And every action it takes is sealed into a tamper-evident, audit-ready record.

> *One platform, both estates, real-time containment, full sovereignty.*

01 KEY BENEFITS

- Protect the production line without taking it offline.
- One platform watches both your IT and your OT estate.
- Threats contained in seconds — not investigated for hours.
- Understands the sequence, not just the alert.
- Legacy equipment protected without re-engineering it.
- Tamper-evident audit trails, ready for regulators and insurers.

02 FEATURE SPOTLIGHT

Speaks your plant's languages

Drops onto the OT you already run — nothing to rip out or replace.

Sees the whole attack, not just the alarm

Shows exactly which cells, lines or sites a compromise can reach, so you contain the right thing.

Learns the rhythm of your operation

Flags the activity that doesn't belong — even when no signature has ever seen it before.

Quantum-safe from day one

Protects your estate against "harvest now, decrypt later" — without a multi-year migration.

DEPLOYMENT

Sovereign and on-premise by default — real-time defence for OT that must never go offline.

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 — and the two halves talk to each other. 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 IT and OT estate, learns what normal looks like, and recognises what doesn't belong — then contains it autonomously, at machine speed, before it reaches the line.
- **Sovereign** means it runs entirely inside your estate, in your jurisdiction, on your hardware — nothing leaves, nothing depends on a foreign service.
- 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 your sites, sensors, control systems and operators is encrypted with post-quantum key exchange — so traffic an adversary harvests today can't be decrypted later when quantum computers arrive ("harvest now, decrypt later").
- Protects legacy 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 project.

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 YOUR ESTATE

- **Detection and encryption defend the line as one system, not two tools.**
- **Your operational traffic stays private — today and against tomorrow's quantum threat.**
- **Legacy OT gets quantum-safe protection without being ripped out or rebuilt.**
- **A single sovereign platform to deploy, run and answer to regulators for.**

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