HIVESTØRM

STORM PLATFORM

PHARMACEUTICALS & BIOTECHNOLOGY / SECTOR

PRODUCT DATASHEET

INTELLECTUAL PROPERTY TO PRODUCTION LINE · DATA INTEGRITY · POST-QUANTUM · SOVEREIGN BY DEFAULT

THE PROBLEM

Pharma and biotech run on secrets — drug formulations, clinical trial data, genomic and biological datasets, decades of R&D — and they are prime targets for nation-state and competitor espionage. A single exfiltration can erase a multi-billion-dollar research lead.

Two estates are under attack at once: the research and IT side, where the IP lives, and the manufacturing and lab floor, where bioreactors, fill-finish lines, instruments and cleanroom controls act at machine speed. A compromise on the production side doesn't just stop a batch — it can threaten patient safety.

Much of the manufacturing estate is validated, long-lived equipment that can't simply be patched or re-architected without re-validation.

And records must be complete, attributable and tamper-evident — while encrypted IP and trial data harvested today can be decrypted once quantum computing matures, so your most valuable secrets have a shelf life measured in decades.

THE SOLUTION

HiveStørm puts one engine across the research IT estate and the regulated manufacturing floor. It learns what normal looks like across labs, pipelines and production, surfaces only what is genuinely new, and contains the threat autonomously at machine speed — before IP walks out the door or a batch is tampered with.

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, lab bench to production line — sovereign, quantum-safe, provable.*

01 KEY BENEFITS

- Defend your IP against nation-state and competitor espionage.
- One engine across research IT and the manufacturing floor.
- Threats contained in seconds — before IP leaves or a batch is tampered with.
- Understands the sequence, not just the alert.
- Your research and patient data never leaves your control.
- Tamper-evident, audit-ready records for regulators.

02 FEATURE SPOTLIGHT

Watches where the IP lives

Sees where formulations, trial data and genomic datasets are held, and flags exfiltration before it completes.

Sees the whole attack, not just the alarm

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

Drops onto validated equipment

Sits alongside the regulated estate you already run — nothing to rip out, nothing to re-validate.

Quantum-safe from day one

Protects IP and trial data against "harvest now, decrypt later" — without a multi-year migration.

DEPLOYMENT

Air-gapped and on-premise by default — protection for research and production that can't go offline or leak.

COMPLIANCE & ASSURANCE

Built on NIST-standardised post-quantum cryptography, with tamper-evident, audit-ready records that support data-integrity obligations. 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 research lab, the data centre and the manufacturing floor. 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 research IT and your manufacturing OT — labs, pipelines, instruments and production lines — learns what normal looks like, and contains what doesn't belong autonomously, at machine speed, before IP leaves or a batch is touched.
- **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 research systems, data stores, instruments and production — is encrypted with post-quantum key exchange, so IP and trial data harvested today can't be decrypted later ("harvest now, decrypt later").
- Protects validated legacy equipment in place: a drop-in post-quantum layer sits in front of instruments and controllers that can't speak modern cryptography, with no re-validation [confirm].
- Quantum-safe from day one — not waiting on a multi-year migration across the estate.

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 R&D AND PRODUCTION

- **Detection and encryption defend your IP and your product as one system, not two tools.**
- **Research, trial and patient data stays private — today and against tomorrow's quantum threat.**
- **Validated equipment gets quantum-safe protection without being ripped out or re-validated.**
- **A single sovereign platform with a tamper-evident record of every action.**

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