HIVESTØRM

STORM PLATFORM

AGRICULTURE & AGRITECH / SECTOR

PRODUCT DATASHEET

CRITICAL FOOD INFRASTRUCTURE · FIELD TO PROCESSING PLANT · REAL-TIME CONTAINMENT · SOVEREIGN BY DEFAULT

THE PROBLEM

Food and agriculture are critical national infrastructure — the systems a country cannot do without — and they are increasingly targeted, by ransomware crews and nation-state actors who treat disruption to the food supply as leverage.

Modern farms and food production run on connected operational technology: autonomous tractors and harvesters, GPS/GNSS guidance, precision-ag sensors and drones, automated irrigation and climate control, grain stores, livestock systems, and downstream processing and cold-chain — much of it across remote sites on intermittent connectivity. A single compromise can stop a harvest, spoil produce, idle a processing line, or misguide autonomous machinery.

The machinery and control systems at risk are long-lived and rarely patched, and remote sites often run with little or no security on hand — refresh cycles measured in seasons and decades, not sprints.

And the data agritech runs on — yield, soil, genetics, breeding and supply-chain data — is valuable IP. Encrypted data and control traffic harvested today can be decrypted once quantum computing matures, so what crosses your networks now has a shelf life measured in decades.

THE SOLUTION

HiveStørm puts one engine across the operation's IT and OT estate — from field machinery and sensors to irrigation, grain stores and the processing plant. It learns the normal rhythm of the season and the line, surfaces only what is genuinely new, and contains the threat autonomously at machine speed — before it can reach the physical process — and keeps protecting a remote site even when its link drops.

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

> *One engine, field to processing plant — sovereign, real-time, provable.*

01 KEY BENEFITS

- Defend critical food infrastructure against ransomware and nation-state disruption.
- One engine across IT, field OT and the processing plant.
- Threats contained in seconds — before they reach the physical process.
- Keeps protecting remote sites even when connectivity drops.
- Your operational and agritech data never leaves your control.
- Tamper-evident, audit-ready records for regulators and buyers.

02 FEATURE SPOTLIGHT

Speaks the farm's and plant's protocols

Reads agricultural and industrial control protocols (ISOBUS / CAN bus, Modbus, OPC UA, MQTT) at wire rate [confirm] — nothing to rip out or replace.

Sees the whole attack, not just the alarm

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

Learns the rhythm of the season and the line

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

Quantum-safe from day one

Protects machine identity, control links and agritech data against "harvest now, decrypt later" — without a multi-year migration.

DEPLOYMENT

Air-gapped and on-premise by default, edge-capable for remote sites — real-time defence that keeps working when connectivity drops.

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 field, the remote site and the processing plant. 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 — field machinery, sensors, irrigation and climate control, grain stores and the processing plant — learns what normal looks like, and contains what doesn't belong autonomously, at machine speed, before it reaches the physical process.
- **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 at a remote site even when the link to head office 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 machines, sensors, sites and the plant — is encrypted with post-quantum key exchange, and every machine's identity is cryptographically bound, so control traffic harvested today can't be decrypted later and commands can't be forged ("harvest now, decrypt later").
- Protects legacy machinery and control kit 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 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 THE OPERATION

- **Detection and encryption defend the operation as one system, not two tools.**
- **Your operational and agritech data stays private — today and against tomorrow's quantum threat.**
- **Legacy machinery 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