HIVESTØRM

STORM PLATFORM

DEFENCE & AEROSPACE / SECTOR

PRODUCT DATASHEET

DATA CENTRE TO FORWARD EDGE · DOCTRINE-BOUND · POST-QUANTUM · SOVEREIGN BY DESIGN

THE PROBLEM

Defence operators face state-level adversaries with state-level patience. Mission systems, command-and-control and classified workloads are targeted relentlessly, and commercial detection tooling built for a different threat model cannot defend them.

Weapons systems, autonomous platforms and the operational technology beneath them now act at machine speed — and adversaries aim squarely at the gap where the operator is squeezed out of the decision.

Encrypted traffic harvested today can be decrypted once quantum computing matures, so the data crossing your networks now has a shelf life measured in decades.

And every defence must be sovereign, kept in customer jurisdiction, and defensible long after the engagement.

THE SOLUTION

HiveStørm is a sovereign engine that hardens the data centre and extends to the airframe, the vessel and the operator's hand-held. It recognises what belongs in the environment, routes only the genuinely new to AI, and enforces an authorised response at machine speed — operator-in-loop where doctrine requires.

It runs air-gapped and on-premise by default, protects every link with post-quantum cryptography, and seals every machine decision into a tamper-evident record under your sole custody.

> *One engine, data centre to forward edge — sovereign, doctrine-bound, defensible.*

01 KEY BENEFITS

- Defend mission systems against state-grade adversaries.
- Understands the sequence, not just the alert.
- Machine-speed response — operator in the loop where doctrine requires.
- Your classified data never leaves your control.
- Quantum-safe today, against tomorrow's decryption.
- A tamper-evident record of every machine decision.

02 FEATURE SPOTLIGHT

Reaches the forward edge

Air-gapped agents extend the same defence to the airframe, the vessel and the hand-held.

Fuses the tactical picture

Radar, RF and EO/IR come together so the decision is made on one view, not five.

Acts within doctrine, every time

Rules of engagement enforced at machine speed, never beyond authorised limits.

Sees the whole attack

Maps what a compromise can reach across the mission, so you contain the right thing.

DEPLOYMENT

Air-gapped and on-premise by default — sovereign custody, no foreign disclosure exposure.

COMPLIANCE & ASSURANCE

Sovereign custody, customer jurisdiction, no foreign disclosure exposure. Built on NIST-standardised post-quantum cryptography.

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 — in the data centre and across the tactical link. 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 from the enterprise to the forward edge, learns what normal looks like for the mission, and contains what doesn't belong — autonomously, at machine speed.
- **Sovereign** means it runs inside your estate, in your jurisdiction, on your hardware — no foreign service, no disclosure exposure.
- Response is doctrine-bound: enforced at machine speed where doctrine permits, operator-in-loop where doctrine requires.

PILLAR B

POST-QUANTUM DEFENCE

PROTECT DATA IN TRANSIT

- Every link — between mission systems, command nodes, platforms and operators — is encrypted with post-quantum key exchange, so traffic harvested today can't be decrypted later.
- The cryptographic spine extends to the tactical edge over air-gapped agents, protecting data in transit even in contested, denied or intermittent conditions.
- Command-and-control channels are cryptographically bound to operator identity — tamper-evident, with every key issuance and rotation sealed.

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, it triggers the cryptographic layer to re-key the affected channels in seconds. The defence moves with the adversary, not against a calendar.

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

04 WHAT THIS MEANS FOR YOUR MISSION

- **Detection and encryption defend the mission as one system, not two tools.**
- **Classified traffic stays protected — today and against tomorrow's quantum threat.**
- **The same engine defends the data centre and the forward edge.**
- **A sovereign platform with a tamper-evident record of every decision.**

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`), anchored in a sovereign HSM, with zero foreign dependencies.

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