HIVESTØRM

STORM PLATFORM

FINTECH & FINANCIAL MARKETS / SECTOR

PRODUCT DATASHEET

CRITICAL NATIONAL INFRASTRUCTURE · QUANTUM-RESISTANT SETTLEMENT · MARKET THROUGHPUT · AUDIT-READY & SOVEREIGN

THE PROBLEM

Banking and capital markets are critical national infrastructure, and they are under nation-state attack. Adversaries generate unique malware per target, automate reconnaissance, and move faster than an alert-and-triage SOC can respond.

Settlement, identity verification and transaction integrity all rest on cryptography that quantum computing will break — and encrypted financial data harvested today, from positions to instructions to identities, can be decrypted later.

Meanwhile every control must satisfy regulators: provable, tamper-evident, and defensible under scrutiny.

THE SOLUTION

HiveStørm protects financial infrastructure as one engine: it recognises normal market and system activity, surfaces only what's genuinely new, and contains threats autonomously at the throughput the markets demand.

It secures settlement, identity and transaction integrity with post-quantum cryptography, and seals every action into a tamper-evident, audit-ready record.

> *Quantum-resistant settlement and integrity — at market speed.*

01 KEY BENEFITS

- Defend market infrastructure against nation-state adversaries.
- Threats contained at machine speed, at market throughput.
- Settlement and transactions protected against the quantum threat.
- Identity and integrity you can prove, not just assert.
- A tamper-evident, audit-ready trail of every action.
- Understands the sequence, not just the alert.

02 FEATURE SPOTLIGHT

Built for throughput

Detection that keeps pace with market-rate data, not a sample of it.

Protects the transaction, not just the perimeter

Settlement and identity secured end-to-end.

Audit-ready by design

Every action sealed as tamper-evident evidence.

Quantum-safe from day one

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

DEPLOYMENT

Data centre, private cloud, or sovereign hybrid — deployed where your data and your regulators require.

COMPLIANCE & ASSURANCE

Built on NIST-standardised post-quantum cryptography, with tamper-evident, audit-ready records of every action. Deployed in your jurisdiction, under your control.

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 — at market throughput. 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 the institution, learns normal market and system behaviour, and contains what doesn't belong — autonomously, at machine speed, without an analyst queue.
- **Sovereign** means it runs inside your estate, in your jurisdiction — nothing leaves, nothing depends on a foreign service.
- Extended detection and response engineered for market-rate throughput.

PILLAR B

POST-QUANTUM DEFENCE

PROTECT DATA IN TRANSIT

- Settlement messages, transaction data and identity records are encrypted with post-quantum key exchange — so financial data harvested today can't be decrypted later.
- Transaction and identity channels are cryptographically bound and sealed, so integrity can be proven, not just claimed.
- Quantum-safe from day one — no 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, it triggers the cryptographic layer to re-key the affected channels in seconds. Cryptography that rotates on threat signal, not on the calendar.

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

04 WHAT THIS MEANS FOR THE INSTITUTION

- **Detection and encryption defend the transaction as one system.**
- **Settlement and identity stay protected — today and against the quantum threat.**
- **Integrity you can prove to a regulator, sealed at every step.**
- **One sovereign platform at the throughput the markets demand.**

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