HIVESTØRM

STORM PLATFORM

MINING & METALS

/ SECTOR

PRODUCT DATASHEET

STRATEGIC RESOURCES · PIT TO REFINERY · REAL-TIME CONTAINMENT · SOVEREIGN BY DEFAULT

THE PROBLEM

Mining and metals supply the raw materials every other industry depends on — increasingly classed as strategic resources — and a compromise that halts a mine or a smelter costs millions a day and can ripple through a national supply chain. Adversaries know it.

The estate spans remote pits, processing plants and refineries, where autonomous haulage, crushing and flotation circuits, and smelter and furnace controls act at machine speed on networks where IT and OT converged long ago. A single compromise can stop production, threaten worker safety — hoists, ventilation, tailings monitoring — or take a site offline.

The equipment is often long-lived industrial control kit, on sites with intermittent, satellite-backhauled connectivity, that can't simply be patched or re-architected.

And metallurgical know-how, exploration data and production records harvested today can be decrypted once quantum computing matures, so the data leaving your sites now has a shelf life measured in decades.

THE SOLUTION

HiveStørm puts one engine across the corporate IT estate and the OT from pit to refinery. It learns the normal rhythm of extraction, processing and smelting, surfaces only what is genuinely new, and contains the threat autonomously at machine speed — before it can halt production or reach a safety system. It runs sovereign and keeps protecting a remote site even when its link to head office drops.

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

> *One engine, pit to refinery — sovereign, real-time, provable.*

01 KEY BENEFITS

- Defend strategic resource production against nation-state adversaries.
- One engine across remote sites, processing and refining.
- Threats contained in seconds — before production stops or a safety system is reached.
- Understands the sequence, not just the alert.
- Your exploration and production data never leaves your control.
- Tamper-evident, audit-ready records for regulators.

02 FEATURE SPOTLIGHT

Defends the remote site

Runs sovereign at pit, plant and refinery, and keeps protecting even when the satellite link to head office drops.

Sees the whole attack, not just the alarm

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

Learns the rhythm of the operation

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

Quantum-safe from day one

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

DEPLOYMENT

Air-gapped and on-premise by default — real-time defence for remote sites and processing that can't 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 — across the pit, the processing plant and the refinery. 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 corporate IT and your site OT — pits, autonomous fleets, processing circuits and smelters — learns what normal looks like, and contains what doesn't belong autonomously, at machine speed, before production stops or a safety system is touched.
- **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 when a remote link 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 sites, control systems, autonomous equipment and head office — is encrypted with post-quantum key exchange, so traffic harvested today can't be decrypted later ("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 across remote and connected sites.

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 exploration data 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 that keeps protecting even when the link to a remote site drops.**

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