HIVESTØRM

STORM PLATFORM

ENERGY & UTILITIES

/ SECTOR

PRODUCT DATASHEET

CRITICAL NATIONAL INFRASTRUCTURE · GENERATION TO GRID EDGE · REAL-TIME CONTAINMENT · SOVEREIGN BY DEFAULT

THE PROBLEM

Energy and water are the infrastructure every other sector depends on, and they are under sustained nation-state attack. Adversaries pre-position inside grid and utility networks to hold the option of disruption.

Generation plants, substations and the control systems beneath them act at machine speed, on networks where IT and OT converged long ago. A single compromise can trip a substation, black out a region, or take water treatment offline.

The equipment at risk is often legacy industrial control kit that cannot simply be patched or re-architected, with refresh cycles measured in decades.

And encrypted operational traffic and grid telemetry harvested today can be decrypted once quantum computing matures — so the data crossing your networks now has a shelf life measured in decades.

THE SOLUTION

HiveStørm puts one engine across the utility's IT and OT estate — from the control room to the substation and the grid edge. It learns the normal rhythm of generation, transmission and distribution, surfaces only what is genuinely new, and contains the threat autonomously at machine speed — before it can reach the physical process.

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, generation to grid edge — sovereign, real-time, provable.*

01 KEY BENEFITS

- Defend critical infrastructure against nation-state adversaries.
- One engine across IT and the OT grid estate.
- Threats contained in seconds — before they reach the physical process.
- Understands the sequence, not just the alert.
- Your operational data never leaves your control.
- Tamper-evident, audit-ready records for regulators.

02 FEATURE SPOTLIGHT

Speaks the grid's protocols

Reads IEC 61850, IEC 60870-5-104, DNP3 and ICCP at wire rate — nothing to rip out or replace.

Sees the whole attack, not just the alarm

Shows which substations, feeders or plants a compromise can reach, so you contain the right thing.

Learns the rhythm of the grid

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

Quantum-safe from day one

Protects grid telemetry and control data against "harvest now, decrypt later" — without a multi-year migration.

DEPLOYMENT

Air-gapped and on-premise by default — real-time defence for control systems that must never 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 control room, the substation and the grid edge. 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 — control rooms, substations, generation and the grid edge — 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.
- 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 control centres, substations, generation plants and field devices — is encrypted with post-quantum key exchange, so grid 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 the grid.

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 UTILITY

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