THE CASE FOR SOVEREIGN DEFENCE IN ENERGY

# Keep the lights on. Keep *control* of the systems that do.

HiveStørm defends the energy infrastructure your business — and your country — depends on, against the threats of today and the quantum era. One platform, run entirely under your control, that detects and stops attacks on its own and keeps your most critical systems trustworthy in real time.

01 WHY WE DO THIS

## Energy is the one thing *everything else depends on.*

A successful attack on an energy operator is not an IT problem with a price tag. It can black out a region, halt production, threaten worker and public safety, and put your organisation at the centre of a national crisis — in hours. That is a board-level risk, and the threat behind it has changed.

The old model of defence — a wall around the network, watched around the clock by a team of analysts — was built for a slower world. The adversaries are now nation-states moving at machine speed. Corporate IT and the operational systems that run the physical grid have merged. The quantum era will break the encryption protecting today's control systems. And most security tools depend on foreign clouds and services — a dependency that, for national infrastructure, is itself the vulnerability.

> *We exist to make the systems a nation can't afford to lose defensible in real time — sovereign, autonomous, and quantum-ready — under their owner's control.*

02 HOW WE DO IT

## One platform. *Not a stack of tools.*

Most organisations bolt together a dozen products from a dozen vendors and staff a team around the clock to watch them. HiveStørm is one engine that does three fused jobs — it understands everything your systems do, detects and stops threats on its own, and protects your data against today's and tomorrow's code-breakers — and it runs entirely inside your walls. Three things make it different, and all three are business advantages, not features:

### Sovereign

It runs on your infrastructure, in your jurisdiction, with no foreign dependency. You own it outright; nothing leaves your estate, and nothing relies on a service you don't control.

### Autonomous

It contains threats in seconds, within the limits you set — so your protection doesn't depend on a large team noticing and reacting in time. Defence at the speed of the attack.

### Quantum-ready now

It protects your data and control links with quantum-safe encryption today — not as a future migration project — closing a gap your competitors are still scoping.

The effect is one platform a leaner team can run, defending your most critical systems at machine speed, proving every decision it makes, and keeping you firmly in control.

03 WHAT IT LOOKS LIKE IN PRACTICE

## A grid operator, *under quiet attack.*

ILLUSTRATIVE SCENARIO

A regional utility runs generation, a control room and dozens of remote substations — some control equipment decades old. *A nation-state group slips in through a trusted supplier.*

| | |
|---|---|
| THE SITUATION | IT and the operational network running the physical grid have grown together over the years. The attacker gains a quiet foothold and begins moving, step by step, toward the systems that control supply. |
| WITHOUT MODERN DEFENCE | Each step looks like ordinary activity on its own. By the time an analyst pieces it together, the attacker is positioned to disrupt supply — and any data they copied can be unlocked later, once quantum computers arrive. |
| WITH HIVESTØRM | The platform has learned the grid's normal rhythm. It recognises the unusual sequence as **one connected attack**, isolates the compromised segment **in seconds without taking the grid offline**, and re-keys the affected links with quantum-safe encryption the moment it senses trouble. Every action is sealed into a tamper-evident record. |
| THE OUTCOME | **Supply stays on.** The attack is contained before it reaches the physical process, the operator can prove exactly what happened to regulators and the board, and the data the attacker took is worthless — today and in the quantum era. |

THE BUSINESS VALUE

## What each leader gets.

FOR THE

### CEO

- Operational continuity and reputation protected from a headline-grade incident.
- A national-infrastructure crisis avoided — and resilience you can speak to with confidence.
- A clear, sovereign answer when customers, government and the board ask "are we safe?"

FOR THE

### CIO & CISO

- One sovereign platform replacing a sprawling, costly toolset of [N] products.
- Far less load on a stretched team — the platform acts on its own within your rules.
- Audit-ready by design, with quantum migration handled rather than deferred.

FOR THE

### Board & Risk

- A demonstrable, defensible security posture — evidence for every decision.
- Reduced regulatory and liability exposure across the estate.
- Resilience that protects enterprise value, financing and continuity of supply.

WHY NOW

**The clock is already running.** Standards bodies require moving off today's encryption between 2030 and 2035, the estimates for when quantum computers can break it keep accelerating, and "harvest now, decrypt later" means data taken today is already at risk. Critical infrastructure carries the longest upgrade cycles of any sector — so for energy, starting now is not early. It is the only way to be ready in time.

NEXT STEP

STEP 01

### Demo

See the platform defend a grid-like environment.

STEP 02

### Exposure report

A passive, no-obligation assessment of where your estate is exposed — nothing installed.

STEP 03

### Bounded proof of concept

A scoped trial in one part of your environment, with success measures agreed up front.