DECENT CYBERSECURITY

Product Portfolio

Sovereign-Grade Post-Quantum Cybersecurity Infrastructure

> *“Securing critical infrastructure for the post-quantum era.”*

14 Products • **Defence-Grade Assurance** • **NATO / EU / National SECRET Clearance**

ISO 9001 | ISO 27001 | ESA-Registered | Quantum-Ready

Sovereign Cybersecurity for Defence, Space, Aviation, Critical Infrastructure & Government

decentcybersecurity.eu

About Decent Cybersecurity

Decent Cybersecurity is a sovereign-grade cybersecurity provider specialising in post-quantum cryptography (PQC), zero-trust architectures, distributed-ledger integrity, and AI assurance for the most demanding operational environments. Our portfolio spans defence, intelligence, space systems, civil aviation, unmanned traffic, critical national infrastructure, and regulated financial sectors.

Vision

To be the trusted sovereign cybersecurity partner of governments, defence forces, space agencies, and critical-infrastructure operators preparing for the post-quantum threat horizon.

Mission

Deliver verifiable, standards-aligned, sovereign-controlled cybersecurity infrastructure, engineered for 20 to 30 year integrity guarantees, NATO/EU interoperability, and operational resilience under quantum-era adversarial conditions.

Credentials & Assurance

Quality Management	ISO 9001 certified
Information Security	ISO 27001 certified
Clearance Levels	NATO SECRET, EU SECRET, National SECRET
Space Sector	European Space Agency (ESA) registered supplier
Cryptographic Posture	Post-quantum ready: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, hybrid modes
Standards Alignment	NIS2, GDPR, NIST PQC, ICAO, EUROCONTROL, EASA, ENISA

Industries Served

- Defence & National Security
- Space Agencies & Satellite Operators
- Civil Aviation, ANSPs & UTM Authorities
- Critical National Infrastructure (energy, water, transport)
- Financial Market Infrastructure & Regulators
- Government, Sovereign Cloud & National PKI
- Law Enforcement & Intelligence Agencies

Product Catalogue

The Decent Cybersecurity portfolio is organised into strategic domains. Each product is sovereign-deployable, post-quantum-ready, and designed to interoperate as part of a unified defence-grade security stack.

01	**PQ-STRAT™**: Post-Quantum Strategic Risk & Threat Framework	GOVERNANCE & RISK
02	**CipherLayer™**: Post-Quantum Trust Layer (Comms & VPN)	PQC COMMUNICATIONS
03	**QuantumProof Protocol™ (QPP)**: Decentralized PQ Communication Fabric	PQC COMMUNICATIONS
04	**CyberFort Blockchain™ (CFB)**: Sovereign Post-Quantum Permissioned Ledger	DISTRIBUTED TRUST
05	**SynapseMesh™**: Sovereign AI Operating System	AI INFRASTRUCTURE
06	**VerityGridAI™**: AI Assurance Infrastructure (TEVV)	AI ASSURANCE
07	**SecureSat Guardian™**: Sovereign Satellite Cybersecurity	SPACE SECURITY
08	**SpaceShield STM™**: Operational Space Traffic Management	SPACE SECURITY
09	**AeroLink™**: Federated Airspace Trust Layer (FATL)	AVIATION & AIRSPACE
10	**DroneCrypt UTM™ (SQ-UTM™)**: Sovereign Quantum-Secure UTM	AVIATION & AIRSPACE
11	**CryptoSleuth Pro™**: Cryptocurrency Forensic Intelligence	FORENSICS & COMPLIANCE
12	**SynapseFire™**: Sovereign Fire Control & Flight Guidance	DEFENCE EFFECTS
13	**PNTMAP™**: Sovereign GNSS Interference & PNT Threat Intelligence	PNT INTELLIGENCE
14	**Security Signal™**: Curated Open-Source Security Intelligence	SITUATIONAL AWARENESS

01 PQ-STRAT™

GOVERNANCE | RISK FRAMEWORK | SOVEREIGN

pqstrat.com

What it is

PQ-STRAT™ is a sovereign-grade **Post-Quantum Strategic Risk & Threat Framework**, a structured governance and risk model purpose-built for the cryptographic transition era. It is not a scanner or a checklist; it is the strategic decision layer that organisations use to inventory cryptographic exposure, score quantum risk, and govern multi-decade migration roadmaps.

> **Core focus: transition-era risk**
>
> - Cryptographic downgrade attacks during hybrid deployments
> - Hybrid validation errors between classical and PQC primitives
> - PKI lifecycle management across long-lived certificates
> - Harvest-Now-Decrypt-Later (HNDL) exposure of long-confidentiality data

Deliverables

- **Technique & Countermeasure Taxonomy:** structured catalogue of PQ-era attack techniques and matched countermeasures
- **PQRI Scoring:** Post-Quantum Risk Index across 5, 10, 20 and 30-year horizons
- **Sector Modules:** tailored extensions for defence, space, finance, energy, sovereign cloud
- **Governance & Versioning:** auditable, version-controlled risk artefacts

Workflow

Cryptographic Inventory → **Exposure Mapping** → **PQRI Scoring** → **Control Domains** → **Migration Roadmap** → **Verification**

Tiers

Open Access	40 techniques + 40 countermeasures (community / evaluation tier)
Full Framework	1,500 techniques + 1,500 countermeasures, sector modules, governance suite

Audience

- Defence ministries and armed forces
- National space agencies and satellite operators
- National cyber authorities & ENISA-aligned regulators
- Critical infrastructure operators (energy, water, transport)
- Financial market infrastructure
- Sovereign cloud and national PKI providers

02 CipherLayer™

PQC COMMS VPN

cipherlayer.ai

Category

CipherLayer™ is the **Post-Quantum Trust Layer** for sovereign communication and connectivity, designed to replace ageing RSA/ECC-based protections across email, messaging, file transfer, voice/video and network tunnelling.

The two products

CipherLayer Secure Comms	Post-quantum cryptography applied to email, messaging, file transfer, and voice/video communications
CipherLayer VPN	Post-quantum tunnelling: site-to-site VPN, remote access VPN, sovereign overlay networks

The problem CipherLayer™ solves

- RSA and ECC are on a documented expiration trajectory under quantum threat
- Adversaries are already executing Harvest-Now-Decrypt-Later campaigns against high-value traffic
- No dominant sovereign post-quantum trust standard exists at the connectivity layer
- Hyperscalers do not provide sovereign-controlled, clearance-grade PQC infrastructure

Differentiators

- **Sovereign-built:** no foreign dependency, full key sovereignty
- **Invisible deployment:** replaces transport-layer crypto without changing user workflows
- **Crypto-agile:** modular algorithms; safe upgrade path as PQC standards evolve
- **Infrastructure, not an app:** operates at the network and trust layer
- **Fills the hyperscaler gap:** engineered for classified, sovereign and regulated use

Target users

Government, defence, intelligence, diplomatic networks, critical infrastructure operators, sovereign cloud, regulated enterprises.

03 QuantumProof Protocol™

PQC DECENTRALIZED ZERO-TRUST

quantumproofprotocol.com

Category

QPP is a **decentralized post-quantum secure communication protocol**, a quantum-resilient communication fabric that replaces centralised PKI, perimeter defences and classical cryptography with a federated, zero-trust, PQC-native model.

3-Layer Architecture

Layer 1: PQC Cryptographic Core	Lattice and hash-based primitives, hybrid modes, crypto-agility
Layer 2: Decentralized Trust & Integrity	Federated trust establishment, multi-party consensus, integrity validation
Layer 3: Secure Communication Fabric	Quantum-secure key exchange, end-to-end encryption, real-time integrity attestation

Capabilities

- Post-quantum key exchange and end-to-end encryption
- Multi-party trust without a centralised certificate authority
- Federated zero-trust across organisational and national boundaries
- Real-time integrity validation of every communication session

Target environments

- Defence and intelligence networks
- Aerospace and space-ground links
- UTM and unmanned aviation command channels
- Critical infrastructure and Industrial IoT

> **QPP vs CyberFort Blockchain™:** QPP operates at the network and protocol layer (live communications). CyberFort Blockchain™ operates at the ledger and consensus layer (long-horizon distributed integrity records). They are complementary components of the same sovereign stack.

04 CyberFort Blockchain™

PERMISSIONED LEDGER | PQC | SOVEREIGN

cyberfortblockchain.com

Category

CyberFort Blockchain™ is a sovereign-grade, **post-quantum permissioned distributed ledger**, long-horizon cryptographic integrity infrastructure for governments, defence and regulated sectors. It is explicitly not a cryptocurrency, DeFi or retail blockchain.

Threat addressed

- Harvest-Now-Decrypt-Later attacks on archived signed records
- RSA/ECC obsolescence under the quantum timeline (2025 → 2028 → 2030 → 2035+)
- 20 to 30 year data integrity requirements for archives, registries, audit trails

Versus public blockchains

- Identity-bound validators with national or organisational accountability
- Permissioned federation, no anonymous participation
- No token economy, no speculative incentives
- Infrastructure-level deployment (on-prem, sovereign cloud, hybrid)
- Deterministic Byzantine Fault Tolerant finality, not probabilistic

4-Layer Architecture

L1: PQC Core	Post-quantum signatures, hash trees, key management
L2: Permissioned Consensus Engine	Identity-bound BFT consensus with deterministic finality
L3: Identity & Federation Layer	Sovereign and cross-domain federation, validator governance
L4: Integration & API Layer	Application integration, evidence export, regulator interfaces

Threat models addressed (TM-01 → TM-07)

TM-01	Harvest-Now-Decrypt-Later
TM-02	Retroactive signature forgery
TM-03	Centralised log manipulation
TM-04	Multi-authority trust breakdown
TM-05	Cryptographic algorithm obsolescence
TM-06	Insider tampering of records
TM-07	Cross-domain federation failure

15 Use Cases

Defence supply chain integrity • satellite command authorisation logging • space traffic management ledger • UAS flight registry • inter-agency information exchange • classified document timestamping • energy grid event logging • critical-infrastructure audit trails • national digital archives • firmware validation • cross-border regulator federation • zero-trust access logging • procurement integrity • financial settlement records • digital identity registry.

Deployment & engagement

Deployment models	On-premise (air-gapped, SECRET, HSM-backed) • Sovereign cloud (NIS2 / GDPR) • Hybrid federation
Engagement phases	1) Architectural Evaluation Workshop → 2) Deployment Feasibility Assessment → 3) Controlled Pilot Federation → 4) Sovereign-Scale Deployment

05 SynapseMesh™

SOVEREIGN AI | MULTI-AGENT | PQC

synapsemesh.ai

Category

SynapseMesh™ is the **Sovereign AI Operating System**, an end-to-end AI stack engineered for classified and critical environments where data sovereignty, provenance and post-quantum security are non-negotiable.

Problems addressed

- Data leakage from commercial and hyperscaler AI services
- Lack of sovereignty over models, weights, training data and inference logs
- Poor interoperability across coalition and inter-agency boundaries
- Absent secure coordination layer for autonomous and multi-agent AI systems

7-Layer Sovereign AI Stack

1. Sovereign Infrastructure (PQC, air-gapped, hardware-rooted)
2. Secure Data Fabric
3. Sovereign Training & Model Management
4. Inference & Serving
5. Zero-Trust AI Control Plane
6. Federated Intelligence Layer
7. Agent Mesh, multi-agent orchestration

Capabilities

- Sovereign training pipelines with full data and weight custody
- Multi-agent orchestration across domains and missions
- Zero-trust AI access control and policy enforcement
- Post-quantum cryptography: CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+
- Federated intelligence sharing without raw data exposure

Use cases

- Multi-domain military operations
- Intelligence fusion and analysis
- Secure enterprise AI for regulated sectors
- Cross-border coalition collaboration (NATO / EU)

Differentiator: SynapseMesh™ is the only end-to-end sovereign AI stack engineered from infrastructure to agent mesh, NATO/EU clearance-ready, and post-quantum from day one.

06 VerityGridAI™

AI ASSURANCE | TEVV | STANDARDS

veritygridai.com

Category

VerityGridAI™ is **AI Assurance Infrastructure**. It operationalises the Test, Evaluation, Verification and Validation (TEVV) lifecycle for AI systems deployed in high-assurance environments.

> **The AI trust gap it closes**
>
> - **Verifiability:** can the AI's behaviour be evidenced and reproduced?
> - **Interoperability:** does it perform under coalition and cross-domain constraints?
> - **Resilience:** does it hold up under adversarial inputs and drift?
> - **Auditability:** is there a defensible evidence trail for regulators?
> - **Standards alignment:** NATO, EU AI Act, NIST AI RMF, sectoral regulators

Core capabilities

- **Automated TEVV Orchestration:** continuous test, evaluation, verification, validation
- **Interoperability Verification:** coalition and cross-system behaviour testing
- **Standards Mapping Engine:** automated alignment to applicable AI standards
- **Audit-Ready Evidence Generation:** regulator-ready and certifier-ready artefacts

Target sectors

- Defence and security agencies
- NATO and allied bodies
- Regulated critical sectors deploying AI in operational decision loops

07 SecureSat Guardian™

SPACE | TT&C | PQC

securesatguardian.com

Category

SecureSat Guardian™ is **sovereign-grade satellite cybersecurity**, protecting Telemetry, Tracking & Command (TT&C), SATCOM links, payload data, and ground station operations across the full space mission lifecycle.

> **Foundation: TT&C protection**
>
> - **Telemetry integrity:** protect downlinked spacecraft state from forgery and tampering
> - **Tracking anti-spoofing:** defend against false-position injection
> - **Command authentication:** cryptographically authenticate every uplinked command

Capabilities

- TT&C security and command authentication
- Anti-spoofing and replay protection on uplink and downlink
- Sovereign key management with HSM-backed custody
- Post-quantum cryptography across links and payload data
- Secure boot and firmware integrity for spacecraft and ground segments
- Zero-trust ground station operations
- Constellation-readiness and inter-satellite link security
- Anomaly detection and security telemetry

12 Operational Use Cases

Including command-spoofing prevention, anti-jamming response, downlink confidentiality, payload data protection, ground station hardening, supply-chain firmware validation, anomaly forensics, quantum future-proofing, NIS2 compliance for space operators, ITU/ECSS alignment, multi-operator federation, and incident response.

Assurance

Clearance	NATO / EU / National SECRET
Certifications	ISO 9001, ISO 27001
Space registration	ESA-registered supplier
Cryptography	PQC-ready (Kyber, Dilithium, SPHINCS+, hybrid modes)

08 SpaceShield STM™

SPACE TRAFFIC | SSA | CONJUNCTION

spaceshieldstm.com

Category

SpaceShield STM™ is an operational **Space Traffic Management platform** delivering real-time Space Situational Awareness (SSA), conjunction assessment and collision risk prediction across LEO and GEO regimes, engineered PQC-ready for sovereign and coalition operations.

Capabilities

- Conjunction assessment and close-approach analysis
- Real-time SSA data integration from multiple sensor sources
- Collision risk modelling with probabilistic outputs
- Manoeuvre decision support for satellite operators
- Alerts, escalation and operator workflow management
- Regulatory and reporting alignment with national and international frameworks

Operational pipeline

SSA Data Sources → **Object Correlation & Orbit Determination** → **Conjunction Detection** → **Risk Modelling** → **Operator Interface & Alerts**

Audience

- LEO constellation operators
- GEO satellite operators
- National governments and space agencies
- Defence space commands and coalition partners

Assurance

Clearance	NATO / EU / National SECRET
Certifications	ISO 9001, ISO 27001
Space registration	ESA-registered
Cryptography	PQC-ready

09 AeroLink™

AIRSPACE | PQC | FEDERATION

aerolink.dev

Category

AeroLink™ is a **Post-Quantum Secure Airspace Coordination Infrastructure**, a Federated Airspace Trust Layer (FATL) for civil aviation, defence airspace, UTM, and space-ground coordination.

> **Three core pillars**
>
> - **Post-Quantum Cryptography** across all coordination messages and trust artefacts
> - **Zero-Trust Federation** across airspace authorities, operators and platforms
> - **Tamper-Evident Integrity Trails** for every authorisation and coordination event

Audience

- Air Navigation Service Providers (ANSPs)
- Ministries of Defence and military airspace authorities
- UTM authorities and U-Space service providers
- National space agencies
- Systems integrators delivering airspace modernisation programmes

7-Layer architecture (summary)

1. PQC Transport & Key Management
2. Distributed Integrity Ledger
3. Federated Identity & Authorisation
4. Airspace Coordination Services
5. Interoperability & Standards Adapters
6. Operational Telemetry & Audit
7. Human-in-the-Loop Analytical Layer (advisory only)

Deployment models

On-Premise • **Sovereign Cloud** • **Hybrid Federation** • **Air-Gapped**

Standards & alignment

ICAO, EUROCONTROL, EASA, NIS2, NATO interoperability frameworks.

10 DroneCrypt UTM™

UTM PQC U-SPACE

dronecryptutm.com

Category

SQ-UTM™, Sovereign Quantum-Secure Unmanned Traffic Management. DroneCrypt UTM™ is the first operational implementation of the SQ-UTM™ category, securing identity, command and authorisation across drone and unmanned aviation operations.

Threats addressed

- Drone identity spoofing
- Command-and-control (C2) interception and injection
- GNSS spoofing and jamming
- Authorisation tampering across UTM stakeholders
- Quantum-era decryption risk against archived flight data

Three architectural pillars

Sovereign Identity Layer	National-grade drone identity, registration and lifecycle management
Quantum-Secure Communications	Post-quantum protected C2, telemetry and coordination links
Integrity & Authorisation	Blockchain-backed immutable flight authorisation and audit

Capabilities

- Post-quantum-secure C2 and telemetry
- Sovereign drone identity and national registry integration
- Immutable, blockchain-backed flight authorisation ledger
- Zero-trust airspace access control
- Real-time monitoring and incident response

Audience

- Defence and security forces
- ANSPs and aviation authorities
- Critical infrastructure operators using UAS for inspection and surveillance

Compliance

NIS2-aligned • **EU U-Space integration** • **ISO 27001**

11 CryptoSleuth Pro™

FORENSICS AML DEFI

cryptosleuthpro.com

Category

CryptoSleuth Pro™ is an institutional **cryptocurrency forensic intelligence platform**, purpose-built for tracing, analysing and reporting on crypto-asset transactions across public blockchains and decentralised finance.

Target users

- Law enforcement agencies
- Financial regulatory bodies and FIUs
- Banks and financial institutions (compliance / AML)
- Cybersecurity firms supporting investigations
- Legal and compliance teams

Core capabilities

- **Comprehensive Data Integration:** merges public blockchain data with private intelligence feeds from banks, law enforcement and financial agencies
- **Advanced Transaction Analysis:** machine-learning detection of laundering, fraud and illicit-funding patterns
- **Wallet Owner Identification:** correlates anonymised on-chain data with private datasets to surface real-world identities
- **DEX Analysis Toolkit:** traces smart contracts and liquidity pools across decentralised exchanges
- **Regulatory Compliance Tracking:** continuous updates aligned with global AML and sanctions standards
- **Robust Security Framework:** end-to-end encryption, regular audits, intrusion detection
- **Intuitive Reporting Interface:** graph visualisation and customisable reports admissible in legal proceedings
- **Proprietary Blockchain Analytics:** multi-layered, smart-contract-aware algorithms
- **Anonymity-Piercing Technology:** behavioural and pattern-based de-anonymisation
- **Cross-Jurisdictional Tracking:** multi-blockchain, multi-legal-framework investigations

12 SynapseFire™

FIRE CONTROL | AIR DEFENCE | PQC

synapsefire.ai

Category

SynapseFire™ is a sovereign, post-quantum **fire control and flight guidance component** for defeating cruise missiles with low-cost interceptors. It is the fire control specialisation of the SynapseCommand™ platform: a pure software layer that raises magazine depth without adding a dollar to the round.

> **The cost-exchange problem**
>
> - **Cost per threat is low:** mass-produced cruise missiles and one-way attack systems invert the defender's economics
> - **Cost per intercept is high:** exquisite interceptors cannot scale to the size of the threat
> - **Magazine depth is the constraint:** every failed intercept spends a round, and every round spent is capacity an adversary can exhaust
> - **The answer is software:** fire control quality is the cheapest place in the kill chain to buy performance, raising probability of kill across interceptors already in the inventory

Core capabilities

- **Multi-sensor fusion:** Kalman-filtered track fusion across radar, electro-optical and passive RF at 10 Hz; tracks survive single-sensor loss and barrage jamming
- **Engageability for IBCS:** launch windows, engagement quality and salvo recommendations published as open engageability objects to the integrated battle command layer
- **Post-launch flight guidance:** proportional navigation with live corrections at 10 Hz and command latency under 150 ms in the reference implementation
- **Two-person authorization:** weapon release is never autonomous; human authorization is enforced in software and cryptographically recorded
- **Post-quantum by default:** every command and track update signed with NIST-standardized ML-DSA, anchored in the CyberFort Blockchain™ audit chain for non-repudiable evidence
- **Natural-language advisory:** CommanderNL™ lets operators query tracks, sensor health and decisions in plain language; advisory only, never a release path

Modelled single-shot probability of kill

BASELINE SINGLE-SENSOR FIRE CONTROL	SYNAPSEFIRE™ FUSED, AGENT-OPTIMISED
Pk 0.60	**Pk 0.84**

In Monte Carlo simulation, fused, agent-optimised fire control raises modelled single-shot Pk from 0.60 to 0.84 against a manoeuvring cruise-missile-class target. Simulated results; methodology available in the technical white paper.

Closed loop: one engagement, end to end

T+05 · Detect	Radar cues a low, slow, small inbound. Fusion opens a track.
T+25 · Rank	A second inbound. The engagement sequencing agent ranks threats and computes launch windows.
T+60 · Degrade	Barrage jamming takes the radar down. The track survives on EO and passive RF.
T+90 · Authorize	Two-person human authorization. Signed, chained, non-repudiable.
T+120 · Guide	Proportional navigation guides the interceptor to a converging predicted intercept point.
T+240 · Defend	A spoofed guidance command is rejected on signature verification. The fire control chain defends itself.

UNCLASSIFIED · SIMULATED SCENARIO DATA

Eight-agent fire control chain

Track Fusion • **Engagement Sequencing** • **Salvo Economics** • **Guidance** • **Spectrum Watch** • **Integrity Monitor** • **Cyber Deception** • **Audit Chain**

Openness & sovereignty

- **MOSA and open interfaces:** the Government owns the interfaces, with Government Purpose Rights on all deliverables; published track and engagement objects, no proprietary lock
- **Sovereign and hardware-agnostic:** pure software on commodity or hardened compute; no vendor lock, no export entanglement on the software layer
- **Part of a fielded platform:** SynapseFire™ is the fire control specialisation of SynapseCommand™, the company's fielded command and control platform

Maturity & assurance

Maturity	Core fire control components fielded and qualified in an operational programme; classified qualification evidence available to cleared government evaluators through government-to-government channels
Evaluation readiness	Ready for hardware-in-the-loop or synthetic evaluation in 1QFY27
Reference unit cost	Approximately USD 95,000 per fire control unit, with zero cost added per interceptor round
Cryptography	NIST post-quantum: ML-DSA signatures, ML-KEM key establishment; hash-chained CyberFort Blockchain™ audit ledger
Programme standing	NATO SECRET facility security clearance • NSPA registered supplier • NCIA member • NATO DIANA Decision Superiority Challenge 2026 selectee • EU EDF AIDA participant

Audience

Air and missile defence commands, ministries of defence and armed forces, integrated battle command programmes and systems integrators, and allied or coalition partners requiring sovereign, non-proprietary fire control.

> **SynapseFire™ vs SynapseMesh™:** SynapseMesh™ provides the sovereign AI stack and agent orchestration. SynapseFire™ applies that architecture to one time-critical mission: fire control and flight guidance, under human authorisation and post-quantum evidence.

13 PNTMAP™

PNT GNSS ADS-B

pntmap.co.uk

Category

PNTMAP™ is **sovereign PNT threat intelligence**: a live map of GNSS interference, jamming and spoofing affecting UK aviation, derived from ADS-B integrity monitoring across UK-owned ground nodes. It is operated by Decent Cybersecurity Ltd, a UK company within the Decent Cybersecurity group, so the measurement infrastructure, the data and the signing keys all remain under UK control.

The problem it addresses

- GNSS interference against civil and military aviation has moved from rare to routine across European airspace
- Operators learn about jamming and spoofing after the fact, from crew reports rather than from measurement
- Awareness often depends on foreign-operated feeds, and the evidence is rarely signed, so it is hard to rely on for investigation or attribution

How it works

UK ground nodes → **ADS-B integrity** → **Signed ingest** → **Anomaly detection** → **Map, API, alerts**

Core capabilities

- **ADS-B-derived integrity anomaly monitoring:** aircraft-reported navigation integrity is analysed continuously to surface areas where positioning quality degrades
- **Post-quantum signing and transport:** ML-DSA-65 (FIPS 204) signing is live on all current nodes and verified at ingest, with TLS 1.3 and hybrid post-quantum key agreement (X25519MLKEM768, ML-KEM / FIPS 203) for supporting clients
- **Verifiable completeness:** per-node ingest commitments are published so reporting gaps are detectable rather than silent, and observations are anchored for later third-party verification

Deployment status

Network	Phase 1 deployment, 2 of 20 planned nodes online
ADS-B anomaly monitoring	Live
ML-DSA telemetry signing	Live on all current nodes
Evidence anchoring	Live
Not yet live	Direct RF sensing; automated event lifecycle, currently operator-curated; commercial API SLA and pricing
Classified deployment	Separate scoped engagement, not the public platform

Audience

Civil aviation authorities, ANSPs and airline operations centres, ministries of defence and military airspace authorities, UAS and U-Space operators exposed to GNSS denial, critical infrastructure operators dependent on GNSS timing, and government bodies requiring sovereign PNT situational awareness.

Scope and limitations. PNTMAP™ is an intelligence and situational-awareness service, not an authorised navigation source, and must not be the sole basis for flight planning, navigation or aviation safety decisions. Monitoring covers only airspace within reception range of commissioned nodes; absence of data elsewhere is not evidence of nominal conditions. PNTMAP™ is not a NATO or NATO DIANA programme and is not endorsed, certified or accredited by NATO.

14 Security Signal™

OSINT | MULTILINGUAL | SITUATIONAL AWARENESS

securitysignal.com

Category

Security Signal™ is a **curated open-source intelligence platform** for security, defence and cyber threats. It continuously gathers reporting, legislative and regulatory activity, and vulnerability disclosure across European sources, then filters, classifies and summarises each item so that teams receive one readable picture instead of a stream they cannot process. Signal instead of noise.

The problem it addresses

- Relevant reporting is fragmented across dozens of national sources in languages a team may not read
- Threat awareness and regulatory awareness live in separate tools, so operational and compliance pictures drift apart
- Commercial feeds add volume rather than reducing it, and rarely reflect national context
- Small security teams cannot sustain manual monitoring across multiple jurisdictions

Core capabilities

- **Multilingual national coverage:** sources are tracked across a portfolio of country domains, so a development in one jurisdiction reaches the team in the language they work in
- **Three streams in one place:** media reporting, legislative and regulatory activity, and disclosed vulnerabilities are collected into a single feed
- **AI-assisted curation:** items are classified, scored for relevance and summarised before delivery, so the platform reduces reading volume rather than adding to it
- **Sector and country filtering:** the picture can be narrowed to the domains and jurisdictions an organisation actually operates in
- **Terminal-style interface:** a dense, keyboard-driven reading surface designed for analysts working through volume, not casual browsing

Use cases

- **Critical infrastructure operators:** track threats, incidents and regulatory movement affecting energy, transport, water and telecommunications in the countries of operation
- **Compliance and regulatory teams:** follow NIS2 and related national implementations as they develop, across multiple jurisdictions at once
- **Security operations:** catch disclosed vulnerabilities relevant to the estate alongside the reporting and advisories that give them context
- **Government and defence staff:** maintain a standing open-source picture without dedicating analysts to manual collection

Audience

- Critical infrastructure operators and their security teams
- National authorities, regulators and government bodies
- Defence and security organisations requiring open-source situational awareness
- Compliance officers working across multiple national regimes

Security Signal™ vs CryptoSleuth Pro™: Security Signal™ operates on open sources to maintain a standing picture of the threat and regulatory environment. CryptoSleuth Pro™ operates on transaction data to investigate a specific case. One tells you what is happening, the other tells you what happened.

The Integrated Decent Cybersecurity Stack

All fourteen products are designed to operate independently, and to compose into a single sovereign defence-grade architecture spanning governance, communications, AI, space, airspace, effects, awareness and forensics.

How the products compose

Govern	**PQ-STRAT™** defines the post-quantum risk model and migration roadmap that drives adoption of every other product in the stack.
Communicate	**CipherLayer™** protects sovereign communications and connectivity. **QuantumProof Protocol™** provides the decentralised PQ communication fabric for federated and zero-trust environments.
Record	**CyberFort Blockchain™** provides 20 to 30 year tamper-evident integrity for authorisations, registries, archives and audit trails.
Reason	**SynapseMesh™** delivers the sovereign AI operating system; **VerityGridAI™** provides the assurance and TEVV evidence layer for every AI system in operation.
Operate Space	**SecureSat Guardian™** protects satellites and TT&C; **SpaceShield STM™** delivers operational space traffic management.
Operate Airspace	**AeroLink™** federates trust across airspace authorities; **DroneCrypt UTM™** secures unmanned operations end-to-end.
Sense	**PNTMAP™** measures GNSS interference against real air traffic, turning positioning degradation into signed, verifiable evidence.
Defend	**SynapseFire™** applies the sovereign AI architecture to fire control and flight guidance, raising intercept performance across interceptor inventories already in the field, under human authorisation and post-quantum evidence.
Watch	**Security Signal™** maintains the standing open-source picture of threat, incident and regulatory activity that frames every other decision in the stack.
Investigate	**CryptoSleuth Pro™** provides the forensic intelligence layer for financial crime, sanctions enforcement and illicit-finance tracing.

Common architectural principles

- **Sovereign by design:** full key, data and operational custody under the customer's jurisdiction
- **Post-quantum native:** Kyber, Dilithium, SPHINCS+, hybrid modes; crypto-agile upgrade paths
- **Zero-trust:** identity-bound, continuously verified access at every layer
- **Standards-aligned:** NATO, EU, NIS2, GDPR, ICAO, EUROCONTROL, EASA, NIST PQC, ENISA
- **Deployable air-gapped:** on-premise, sovereign cloud, hybrid federation, classified enclaves
- **Auditable:** every product produces evidence artefacts suitable for regulators and certifiers

Engagement Model

Decent Cybersecurity engages with sovereign and regulated customers through a structured, low-risk progression designed to validate fit before scale.

Phase 1: Architectural Evaluation	Workshop to map customer environment, threat horizon and applicable products from the portfolio.
Phase 2: Feasibility Assessment	Deployment feasibility, integration analysis, sovereign-control review, regulatory mapping.
Phase 3: Controlled Pilot	Bounded operational pilot, typically a single product or federated subset, with measurable success criteria.
Phase 4: Sovereign-Scale Deployment	Full operational rollout, federation onboarding, lifecycle support and crypto-agility maintenance.

Contact

Decent Cybersecurity engages directly with governments, defence ministries, space agencies, ANSPs, national regulators and qualified critical-infrastructure operators.

Website	`decentcybersecurity.eu`
Portfolio domains	`pqstrat.com` • `cipherlayer.ai` • `quantumproofprotocol.com` • `cyberfortblockchain.com` • `synapsemesh.ai` • `veritygridai.com` • `securesatguardian.com` • `spaceshieldstm.com` • `aerolink.dev` • `dronecryptutm.com` • `cryptosleuthpro.com` • `synapsefire.ai` • `pntmap.co.uk` • `securitysignal.com`
Assurance	ISO 9001 • ISO 27001 • NATO / EU / National SECRET clearance • ESA-registered