

■ EUROPE IS REARMING

ITS SUPPLY CHAINS AREN'T READY. WE'RE FIXING THAT.

THE EVIDENCE LAYER FOR EUROPEAN DEFENCE SUPPLY CHAINS

THE PROBLEM

EVERY GAP IS A LIABILITY YOU ALREADY OWN.

The risk you haven't found isn't the risk that isn't there. It's the risk no one is watching, and the regulator, the auditor and the contract all hold you accountable for it. Unproven origin doesn't just stall payments, it risks exclusion from EU-funded defence programmes and failed audits on live contracts.

01

FRAGMENTED RECORDS

THE GAP

Evidence is split across ERP, PLM, MES, drives and inboxes. No system holds the whole picture, so no one sees the whole risk.

WHAT IT COSTS

An audit that should take an afternoon takes three weeks of manual assembly, and one missing document stalls a milestone payment.

02

NO VISIBILITY PAST TIER 1

THE GAP

Direct suppliers are known. Sub-tier origin, ownership, certification, and export exposure remain unverifiable.

WHAT IT COSTS

A Tier-3 part fails an origin or export check, and you find out when a shipment on a live contract is blocked from leaving.

03

NO LINK: COMPONENT ↔ NETWORK

THE GAP

A single part or supplier can quietly support multiple programmes until one failure stalls all of them.

WHAT IT COSTS

One supplier quietly underpins five programmes. They fail an audit, and all five stall at once.

04

NO PROACTIVE SIGNAL

THE GAP

Certifications, origin shifts and sanctions changes go unwatched until an audit goes looking, months too late.

WHAT IT COSTS

A cert lapsed 40 days ago. You've been shipping non-compliant since, and your EU-origin reporting is already wrong.

— WHY NOW

THREE NEW FORCES THE CURRENT STACK WAS NOT BUILT TO SATISFY.

Together, they create a new category: sovereign, audit-ready supply-chain evidence for European defence.

01

REARM EUROPE · THE MONEY ARRIVED

EU defence expenditure rose from ~€218B in 2021 to ~€343B in 2024. Equipment procurement reached ~€88B in 2024, up ~39% year-on-year. The tools didn't move.

02

SOVEREIGN CLOUD · THE WINDOW JUST OPENED

AWS European Sovereign Cloud went GA in Brandenburg, Germany in January 2026. EU-sovereign enterprise cloud is now commercially available, but there is still no obvious system of record for defence supply-chain evidence built around it.

03

EDIP 2025 · THE ELIGIBILITY GATE

EDIP turns component origin into an eligibility constraint. EU-funded defence actions must keep non-EU / non-associated-country components within a 35% cost cap, creating a new need for auditable, multi-tier evidence. Miss the cap and the action loses EU funding eligibility.

· WHAT EVERYONE'S MISSED

THE PROOF ALREADY EXISTS. NO ONE HAS CONNECTED IT.

Defence teams already hold the records — contracts, POs, BOMs, certificates and supplier declarations. The evidence isn't missing; it's **disconnected**, and today it's **assembled manually**, questionnaire by questionnaire, so the answer is stale the day it's filed and stops at Tier 1. Connect it once and every part, supplier and programme can be traced, gaps become visible, and audit packs replay on demand.

· WHAT CHANGES

THE STATUS QUO

EVIDENCE IS OFTEN ASSEMBLED MANUALLY, QUESTIONNAIRE BY QUESTIONNAIRE. SLOW, STALE AND HARD TO TRACE.

THE REALITY

THE RECORDS ALREADY EXIST ACROSS THE SYSTEMS COMPANIES RUN TODAY. A CONNECTION PROBLEM, NOT A COLLECTION ONE.

THE OPENING

THE FIRST PLATFORM TO CONNECT AND STANDARDISE PROOF BECOMES THE EVIDENCE LAYER BUYERS AND SUPPLIERS RELY ON.

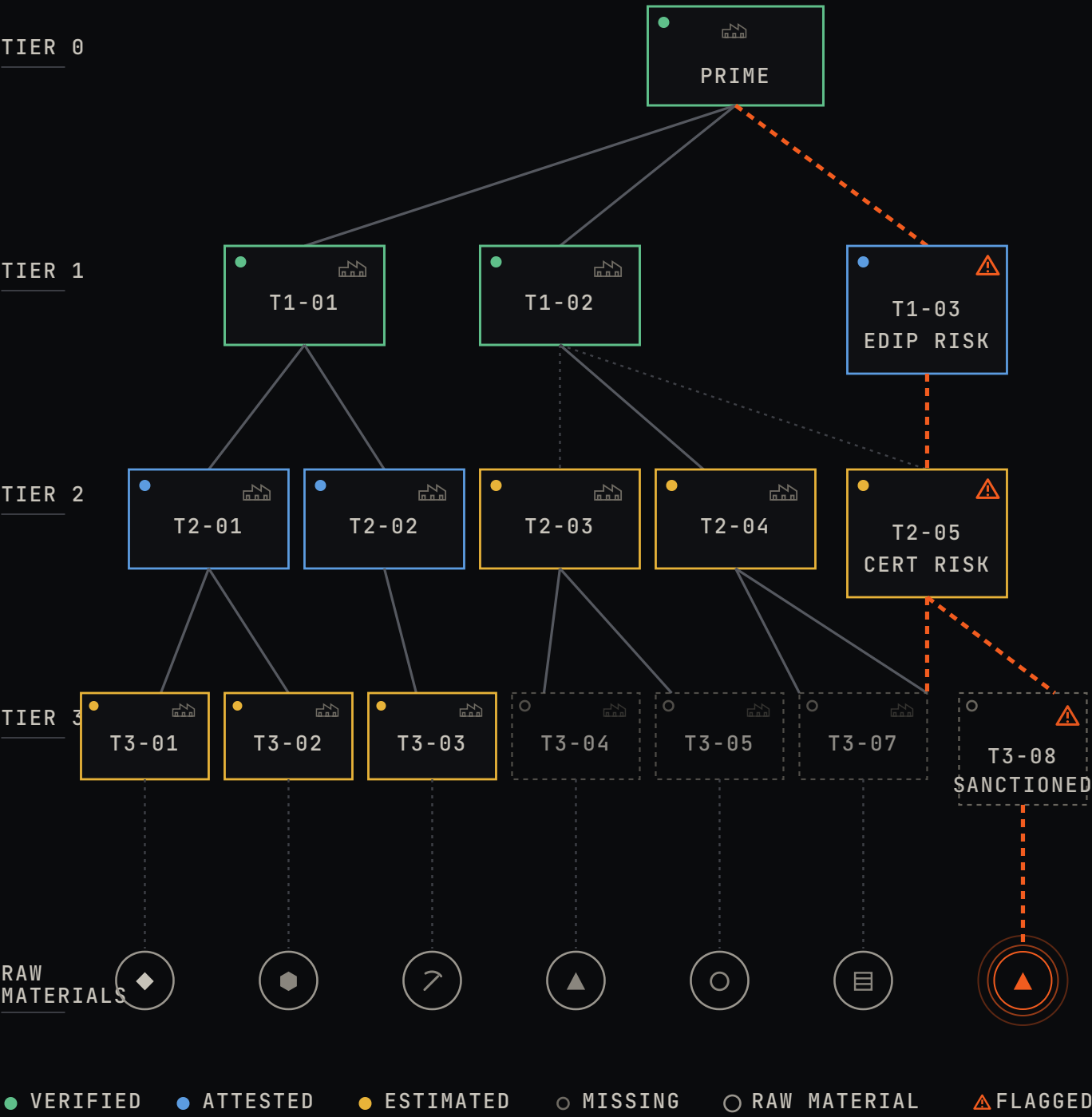
THE WEDGE

WE MAKE EVERY TIER PROVABLE.

Risk and proof both break down beyond Tier 1. DefenceOS connects existing systems, maps what can be proven, and flags every missing, estimated, or unverifiable link.

- **Connect existing systems** — trace from direct suppliers toward raw materials, flagging gaps wherever evidence is missing.
- **Separate proof from assumption** — mark every supplier, part, certificate, and BOM link as verified, attested, estimated, or missing.
- **Propagate risk to programmes** — show which buyers, parts, and programmes are exposed when risk appears anywhere in the chain.

SUPPLIER-COMPONENT EVIDENCE GRAPH · RISK PROPAGATION · CONTINUOUS MONITORING



— THE PRODUCT

ONE PRODUCT. SOURCE RECORD TO AUDIT PACK.

Connect, see and prove aren't three tools — they're three views of one governed evidence graph, where verified, attested, estimated and missing records are kept explicitly apart.

01

CONNECT

Connect ERP, PLM, MES, supplier portals and the records scattered across drives and inboxes. We start read-only; governed write-back is optional and customer-approved, your systems stay the system of record.

DAY-1 DELIVERABLES, DATA-QUALITY HEATMAP · MISSING-EVIDENCE LIST · RISK REGISTER

02

SEE

Your evidence posture appears: EU-origin %, certification gaps, sanctions and export-control exposure. Every figure carries its state — verified, attested, estimated or missing — and traces to a source record.

LIVE VIEW, EVIDENCE GRAPH

03

PROVE

AI never touches the math. Deterministic engines compute every figure; AI only summarises, with citations and missing-support flags. A human approves every compliance output before it ships.

AUDIT DELIVERABLE, REPLAYABLE AUDIT PACK

TRACTION

EARLY, BUT ALREADY TANGIBLE.

WEDGE VALIDATED, BUYER-OWNED DATA FIRST, NO SUPPLIER ACTIVATION FOR DAY-1 VALUE

01 · LIVE

A WORKING PROTOTYPE, NOT SLIDES

Live prototype demonstrates the end-to-end workflow on sample data. Production build underway in parallel.

02 · SHARPENED

BUILT TO LAND FAST

Discovery with four defence-tech investors and operators surfaced the same two adoption barriers, change management and supplier onboarding. We redesigned the initial deployment to deliver value from buyer-owned data before any supplier participation is required.

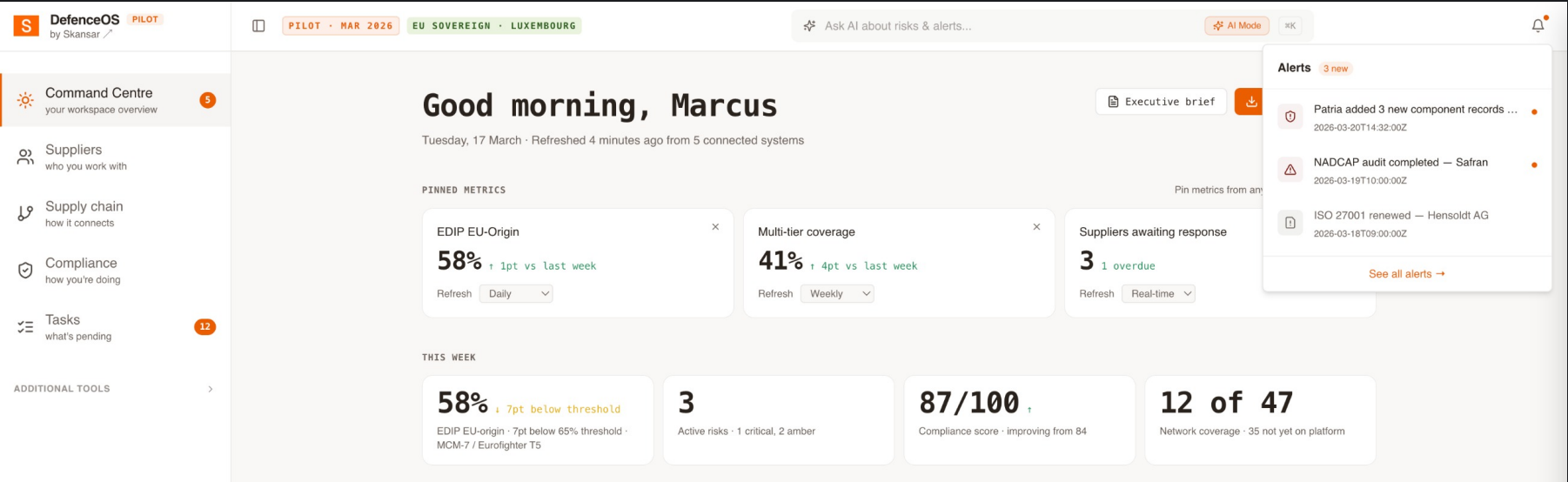
03 · LEAN

BUILDING PRE-FUNDING

Two founders plus one engineering contributor, three total. Zero outside capital to date.

PILOT · COMMAND CENTER

WORKING PROTOTYPE



DISCOVERY VALIDATION · IN-DEPTH INTERVIEW, EX-UK STRATEGIC COMMAND · EX-PWC · AEROSPACE-OEM QUALITY ENGINEER

Pain confirmed

Confirmed the core pain first-hand: beyond Tier 1, visibility disappears, and the evidence that exists sits in disconnected spreadsheets and drives.

Positioning sharpened

Firms run multiple ERPs and treat change management as the hardest barrier. So we connect to existing systems rather than replace them, delivering value from a buyer's own data before any supplier joins.

— MARKET, THE OPPORTUNITY

A MANDATED MARKET WITHOUT A SOVEREIGN EVIDENCE SYSTEM OF RECORD.

Supply-chain risk management is already a multi-billion-dollar software category. EDIP and ReArm Europe add the defence-specific trigger, audit-ready proof of origin, eligibility and security-of-supply. The gap isn't generic risk scoring; it's a sovereign evidence system of record for multi-tier defence supply chains.

~\$9.5_B

SUPPLY-CHAIN RISK MANAGEMENT MARKET BY 2031
~\$5.1B in 2026 · ~13% CAGR
· WHO WE SELL TO

ICP · Primary

TIER-2 / TIER-3 MANUFACTURERS

Components, avionics, materials, 50–500 FTE. Drowning in Prime EDIP requests, we sell compliance automation that helps them win and keep contracts.

~€800_B

REARM EUROPE / READINESS 2030
Defence-spending mobilisation

ICP · Expansion

PRIMES & TIER-1S

Once 50+ of their suppliers are on the platform, we sell Primes network-wide visibility, which pulls in more suppliers.

~2,500₊

DEFENCE-RELATED SMES
Plus primes, mid-caps & procurement bodies

Geographies

DE · BENELUX → FR · NORDICS

Launch DE & Benelux (pilot density); EDIP-eligible EU-27 by year two.

None

EU-SOVEREIGN, DEFENCE-NATIVE
No obvious default today

HOW THIS SCALES
LAND → OWN THE DATA

We land at **EDIP evidence**, then accumulate a verified provenance graph incumbents don't hold, becoming the evidence system of record across EU defence's multi-tier base.
Coverage compounds, not headcount.

— POSITIONING

WHY EXISTING TOOLS DON'T SOLVE THE EDIP EVIDENCE GAP.

DefenceOS does not replace ERP, MES, PLM, risk or data platforms. It connects to them and adds the EU-sovereign, EDIP-native evidence workflow they weren't built to provide by default.

	ERP / MES / PLM SAP · ORACLE · COUPA	SUPPLY-CHAIN RISK PLATFORMS RESILINC · EXIGER · INTEROS	HORIZONTAL DATA PLATFORMS PALANTIR · GENERIC AI	DEFENCEOS EU-SOVEREIGN BY DESIGN
EU DATA SOVEREIGNTY	Sovereignty varies by vendor and deployment; these stay internal systems, not a sovereign cross-company evidence layer.	Often third-country-controlled, which can raise legal-access and procurement-sovereignty concerns for sensitive defence evidence.	Third-country-headquartered; sovereignty depends on bespoke setup, not the default.	EU-sovereign by design: jurisdictional control, access governance, permissioning and evidence lineage, not hosting alone. Accreditation in progress.
CROSS-COMPANY NETWORK EVIDENCE	Authoritative internal records, POs, BOMs, approvals, but company-local, with no cross-company evidence graph.	Strong supplier-network and risk mapping; not packaged by default as an EDIP-origin evidence workflow.	Flexible data foundation; you design the supplier ontology, evidence states and workflows yourself.	No buyer can force every supplier onto one system. DefenceOS connects source records into a cross-company, multi-tier evidence graph; customer systems stay the system of record.
EDIP-NATIVE METHODOLOGY	EDIP handled manually or via bolt-on tools; not a native origin / eligibility workflow.	Best-in-class for sanctions and US trade rules; EDIP origin workflow built from scratch.	A platform, not a prebuilt methodology; you supply the rules and evidence model.	Configurable EU-origin / eligibility calculation, export-control workflows, plus cited AI queries over the EU-resident evidence graph.
AUDITABLE DEFENCE EVIDENCE	Strong internal transaction and change audit trails; not cross-company, EDIP-ready evidence packs.	Risk intelligence first; not packaged as source-linked defence audit evidence by default.	Lineage when configured; not a prebuilt EDIP-native evidence product out of the box.	Every figure traces to a source record, with evidence states (verified / attested / estimated / missing) and replayable audit packs.

— THE MOAT

THE WEDGE GETS US IN. THE MOAT COMPOUNDS.

Sovereignty is the entry. Methodology and evidence gravity are what make us hard to replace once we're in.

01

SOVEREIGNTY INCUMBENTS CAN'T RETROFIT

US-domiciled risk platforms can add EU hosting, but they can't easily undo jurisdictional exposure or a non-sovereign architecture. Defence buyers need sovereignty at the foundation, not as an afterthought. That's our entry wedge.

02

EDIP-NATIVE METHODOLOGY BECOMES WORKFLOW LOCK-IN

As programmes demand stronger proof of origin and eligibility, the winning product isn't another dashboard, it's the methodology. The aim: our EU-origin calculations and audit packs become the trusted operating format, sitting inside programme execution.

03

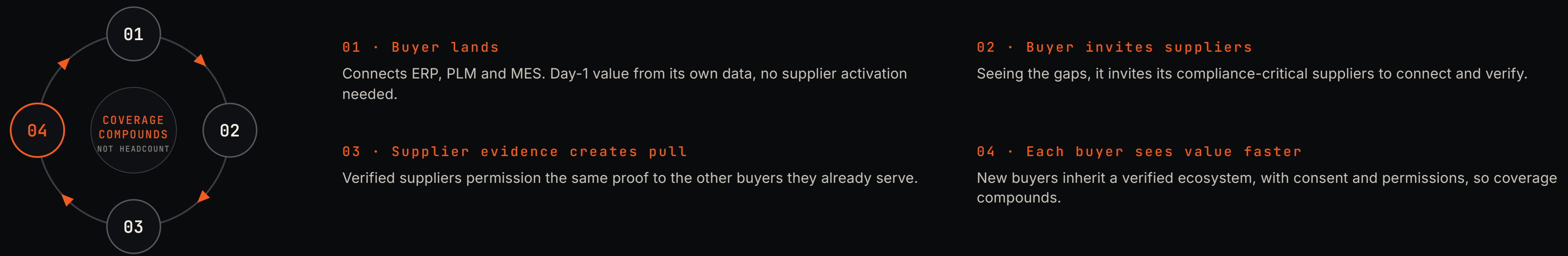
EVIDENCE GRAVITY CREATES DURABLE RETENTION

Once suppliers, parts, BOMs, certificates, risks and approvals are linked into a verified evidence graph, the platform becomes the compliance memory of the organisation. Replacing it means rebuilding the audit trail and re-validating evidence from scratch.

BUSINESS MODEL

HOW DO WE GROW?

THE GROWTH LOOP



DENSITY DRIVER, 5-15 COMPLIANCE-CRITICAL SUPPLIERS PER PROGRAMME.

REVENUE MODEL · ANNUAL SAAS SUBSCRIPTION

Plan · 01 · Essentials

TIER-2 / TIER-3 MANUFACTURERS

€30–50K / YEAR · INDICATIVE

Evidence monitoring, multi-tier traceability, audit-ready packs.

Plan · 02 · Enterprise

PRIMES & PROCUREMENT BODIES

€75–120K+ / YEAR · INDICATIVE

Advanced analytics, cited AI queries, air-gap deployment.

SOFTWARE-CLASS GROSS MARGINS · PRICING TO BE VALIDATED WITH DESIGN PARTNERS

FOUNDING TEAM

ENGINEERS WHO'VE BUILT AT AMAZON SCALE.

The same supply-chain and procurement systems, rebuilt as sovereign infrastructure for European defence.

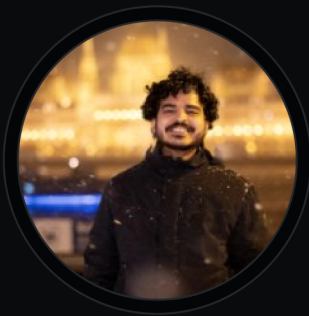


SUBHASISH DAS
CO-FOUNDER · CTO

Built global warehouse and procurement management software at Amazon, the same class of multi-party supply-chain system DefenceOS is now building for defence. Deep expertise in distributed systems, high-reliability data pipelines, and security-focused backend architecture.



- LINKEDIN
- SUBHASISH@SKANSAR.COM



KALPESH SINGH
CO-FOUNDER · CEO

Engineering leader with 10+ years building advanced frontend and user-centric systems. Experienced in leading engineering teams across international environments. Owns commercial strategy and go-to-market.



- LINKEDIN
- KALPESH@SKANSAR.COM

A PHASED PATH TO DEFENCE-GRADE SECURITY.

We start with unclassified and restricted supply-chain data, BOMs, certificates and origin, so no top-secret infrastructure is needed on day one. Accreditation deepens as we move up.

01

FOUNDATION
· MONTHS 1–6

- ISO 27001 certification.
- Deployed on AWS European Sovereign Cloud (Brandenburg, DE).
- Architected for NATO UNCLASSIFIED and EU RESTRICTED data.

02

COMPLIANCE
· MONTHS 6–12

- BSI C5-compatible infrastructure foundation.
- Independent penetration testing.
- Begin national accreditation, e.g. VS-NfD in Germany.

03

CLASSIFIED
· YEAR 2+

- Pursue full national-security accreditation for classified programme data.
- Air-gapped deployment option for prime on-premise requirements.

THE ASK

€2M · 18 MONTHS · FIRST PAYING CUSTOMERS.

≈ 18-MONTH RUNWAY · TO A REPEATABLE PAID-PILOT MOTION + ENTERPRISE SECURITY ACCREDITATION

MILESTONES

Month 03

Connectors production-ready · first design partner in structured conversations · Day 1 value live.

Month 06

Design partners onboarded · LOIs from Tier 2/3 manufacturers · pricing and onboarding model validated.

Month 12

First paid pilots · 5+ manufacturers in active conversations · ISO 27001 audit underway.

Month 18

3–5 paying customers · Tier-1 expansion conversations · commercial hires.

CAPITAL ALLOCATION

60%
PRODUCT & ENGINEERING

→ The deterministic evidence engine and cited-AI query layer, hardened for production.

20%
SECURITY & COMPLIANCE

→ ISO 27001 certification, independent penetration testing, on AWS European Sovereign Cloud (Brandenburg, DE).

BSI C5-compatible infrastructure foundation · full C5 certification on first customer requirement.

20%
GTM & PILOTS

→ Design-partner programme and first commercial & domain hires.

— • IF WE WIN

EVERY EUROPEAN DEFENCE SHIPMENT MOVES ON AN EVIDENCE RAIL WE BUILT.

→ SOVEREIGN BY ARCHITECTURE.
PROVABLE BY DEFAULT.

Stripe became the rail for payments. Plaid for banking.
DefenceOS becomes the rail Europe's defence supply chain runs
on, sovereign, multi-tier, audit-ready by default.

• BUILD IT WITH US

€2M seed

18-MONTH RUNWAY • FIRST PAYING CUSTOMERS

SUBHASISH DAS • CTO

subhasish@skansar.com

KALPESH SINGH • CEO

kalpesh@skansar.com

• WEB

skansar.com

MARKETING

pilot.skansar.com

LIVE PILOT