

■ EUROPE IS REARMING

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

THE AGENTIC EVIDENCE LAYER FOR EUROPEAN DEFENCE
SUPPLY CHAINS.

SITS ON THE SYSTEMS YOU ALREADY RUN.

LIVE PRODUCT app.skansar.com

— THE PROBLEM

WHY DEFENCE SUPPLY CHAINS BREAK DOWN.

The data already exists. Pulling it together is the easy half. Nobody is watching it, so exposure is found during an audit, months after it started.

01 · Reactive

PROBLEMS FOUND TOO LATE

Non-compliance is discovered during audits, months after the exposure started. By then, production, contracts, and reporting are already affected.

02 · Opaque

NO VISIBILITY BEYOND TIER 1

You know your direct suppliers. Beyond that, you have no way to verify who is compliant, who has expired certifications, or who poses a risk.

03 · Scattered

FRAGMENTED RECORDS

Compliance evidence lives in emails, shared drives, and disconnected systems. When an auditor asks for proof, teams spend weeks pulling it together.

IN THEIR WORDS
QUALITY ENGINEER
AIRCRAFT MANUFACTURER

"We know who we buy from. Below that, we see nothing. The documents we have are spread across many spreadsheets and folders."

THE WEDGE

OUR AGENTS WATCH EVERY TIER.

Supply chains break beyond Tier 1. That's where no one is looking, and no one is watching.

- Agents read your ERP and map **every tier**, from direct suppliers down to raw materials. Read-only, no rip and replace.
- They classify certificates and export-control paperwork, and **track sanctions and regulation** as they change.
- When risk appears anywhere, they propagate it to **every buyer and programme** it touches, and surface what needs a decision today.

ONE CONNECTION. NO SUPPLIER ONBOARDING FOR FIRST VALUE.

SUPPLIER GRAPH · LIVE RISK PROPAGATION

LIVE MONITORING

64.6% EU-ORIGIN

EDIP REQUIRES ≥65%, THIS PROGRAMME DOES NOT QUALIFY

YOUR
PRODUCT

Wing actuator assembly
6 parts · 4 suppliers · 3 problems

TIER 1

Bayern Präzision
Germany · proven

Nordic Drive AB
Sweden · no permit

Kraft Lager GmbH
Cert expiring

Vilnius Electronics
Lithuania · proven

TIER 2

Steel billet
Germany · proven

RE-14 Magnet
China · banned owner

Bearing steel
Germany · proven

CN-05 Connector
Origin unknown

RAW
MATERIAL



Rare-earth refiner, four tiers down

● PROVEN

● EXPIRING

● PROBLEM FOUND

--- RISK PATH

THE MOAT

01 · Data gravity

Every supplier connects to 5–15 buyers. Modelled: by customer 30, the graph reaches ~5,000 verified edges. New entrants start at zero.

02 · Network effects

Suppliers bring buyers. Buyers pull in suppliers. Incomplete graphs aren't usable for compliance, the network compounds.

03 · Switching cost

Leaving means re-mapping every supplier and re-auditing from scratch. Defence firms do not do that.

LIGHT TO ADOPT. HARD TO LEAVE.

— TRACTION

LIVE IN PRODUCTION, BEFORE THE FIRST EURO RAISED.

01 · LIVE

FIRST RELEASE LIVE IN PRODUCTION

Real supply-chain workflows running end-to-end, not wireframes.

02 · SECTOR

ACCEPTED INTO TUM VENTURE LABS

Aerospace & Defense, Cyber Security stream. Problem framing confirmed by the sector.

03 · VALIDATED

PRODUCT AND MARKET FIT VALIDATED

Over a dozen operators and investors interviewed to reach this conclusion.

04 · LEAN

BUILDING PRE-FUNDING

Two founders. Zero outside capital to date.

05 · CAPABILITY

AGENTIC EVIDENCE, RUNNING

Document classification, continuous monitoring, and risk propagation across the graph. Not roadmap.

■ COMMAND CENTRE · LIVE

APP.SKANSAR.COM

DefenceOS

by Skansar

Command Centre

what needs your attention today

Supply chain

who you buy from and depend on

Insights

how the business is performing

Evidence

certifications and documents

Value chain

ask questions of your data

Support

Feedback

Ask AI about risks & alerts...

AI Mode

HE

REFRESHED 4M AGO · 5 SOURCE SYSTEMS CONNECTED

AI Assist

Executive brief

Good morning, Elena.

• 3 of 12 programmes need attention. Eurofighter T5 is nearest its audit.

Active risk & insights

CRITICAL

NAV-INS-2201 - Single-source exposure

SUPPLY SECURITY

Review and disposition this risk - act →

CRITICAL

PWR-CU-3300 - Certificate expired

EVIDENCE

40 days lapsed, 2 orders still open - act →

CRITICAL

LOT-T3-559 - No export permit on file

EXPORT CONTROL

Required before the next shipment leaves - act →

22 more in insights →

Across all programmes

PROGRAMMES AT RISK

3 / 12

Need attention - 9 clear

NEAREST AUDIT

12 days

Eurofighter T5 - GDP eligibility

Prepare audit pack →

EVIDENCE MISSING

248 -12

Average 24 critical blockers

AI insight

EU-DR0326 - EUROFIGHTER T5

64.6 %

GDP requires all 5%

Decisions requiring attention - 29 across the portfolio

See all in Tasks →

NEEDS YOUR ACTION - 29

NAV-INS-2201 — Single-source exposure

Eurofighter T5 · Owner: N2210

ESTIMATED

PWR-CU-3300 — Certificate expired

Eurofighter T5 · Owner: PWR06

ESTIMATED

SPB-RD-5510 — Single-source exposure

HR08 · Owner: B46EY

ESTIMATED

LOT-NAV-2026-0442 — Component quality

Eurofighter T5 · Owner: N2210

VERIFIED

LOT-PWR-2026-0110 — Component quality

Leopard 2A8 · Owner: P0804

ATTENDED

LOT-SPB-2026-0511 — Component quality

Patria 600 L4 · Owner: B46EY

MISSING

SINGLE-SOURCE - CRITICAL

NAV-INS-2201 — Single-source exposure

Eurofighter T5 - Supplier N2210 - Owner: N2210

NEXT BEST ACTION

Resolve it, or mark it not impactful, before it escalates further.

Review this risk.

RHY

• One qualified source for this part, used in 5 programmes.

• If it stops, all five stop together. Source: N2210.

YINELINE

• Mitigation window - 21 days

30 JUL 2026 - 1 step the system can auto-run

• Risk detected on N2210 - Tier 0

20 JUL 2026 - note single-source

COMPUTED BY DETERMINISTIC RULES. AI EXPLAINS AND SUMMARISES, IT NEVER COMPUTES.

■ SEE IT LIVE | → app.skansar.com

 MARKET, A WINDOW OPENED

THREE POLICY MOVES OPENED THE WINDOW.

EDIP regulation. ReArm Europe. EU-sovereign cloud, now a reality. Together they force every defence buyer to prove a clean supply chain, and none of the three has a default vendor. The window closes when incumbents wake up.

€418_B

EU-27 DEFENCE SPEND 2025

+20% in one year · €454B in 2026

€800_B

REARM EUROPE · MOBILISATION TARGET

Incl. €150B SAFE loans · by 2030

€115_B

EQUIPMENT PROCUREMENT 2025

+26% in real terms from 2024

2,500₊

DEFENCE SMES IN EU

Multi-tier supplier base

· WHO WE SELL TO

ICP · Primary

TIER-2 / TIER-3 MANUFACTURERS

Components, avionics, guidance, materials, 50–500 FTE, supplying EU primes.

ICP · Expansion

PRIMES & PROCUREMENT BODIES

Pull-through from Tier-2 adoption. Multi-tier visibility for programme owners.

Geographies

DE · BENELUX → FR · NORDICS

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

REGULATION

(EU) 2025/2643

The **European Defence Industry Programme** makes multi-tier supply chain provenance a condition of EU programme funding. No system exists to prove it.

POSITIONING

WHY NOT EXISTING TOOLS?

DefenceOS does not replace these systems. It connects to them and adds the agentic evidence layer none of them provides.

· Why don't primes build this themselves? They've tried. The data lives outside their walls, across hundreds of suppliers. Network effects compound off-prime, not inside one.

	LEGACY ERP / MES SAP · ORACLE · COUPA	NON-EU RISK PLATFORMS RESILINC · EXIGER · INTEROS	DEFENCEOS EU-SOVEREIGN · AGENTIC LAYER
PROACTIVE DETECTION	Nothing watches. Exceptions surface when someone goes looking.	Risk scores and dashboards. A human still has to read them and decide.	Autonomous agents monitor continuously and surface the decision with the reason attached. Figures underneath are computed deterministically, so an AI conclusion is defensible to a regulator.
EU DATA SOVEREIGNTY	Often non-EU hosting and limited control over CLOUD Act exposure.	US-domiciled and CLOUD Act exposed. A structural barrier to serving EU-funded defence programmes.	EU-first hosting architecture, designed to avoid non-EU CLOUD Act exposure, with Member-State data residency options.
MULTI-TIER TRACEABILITY	Site-centric systems with limited cross-supplier visibility.	Strong multi-tier mapping, but built for US regulations. No EDIP EU-origin calculation.	Purpose-built for multi-tier supplier networks and cross-programme visibility.
EDIP COMPLIANCE	Manual, spreadsheet-driven, or bolt-on compliance tools.	Anchored on UFLPA and US trade rules. EDIP workflows would need building from scratch.	Native EDIP EU-origin calculation, plus EU, national, and ITAR/EAR export-control workflows.

— BUSINESS MODEL

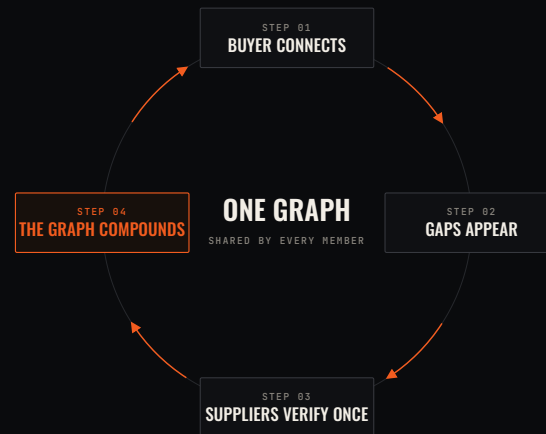
HOW WE GROW.

· THE NETWORK LOOP

- 01 **Buyer connects.** Points DefenceOS at the ERP it already runs. Value on day one from its own data, with no supplier needed to make it work.
- 02 **Gaps appear.** The buyer sees what it cannot prove, and invites the suppliers behind those gaps.
- 03 **Suppliers verify once.** A supplier proves itself once, and that proof serves every buyer sourcing from it.
- 04 **The graph compounds.** Each verified edge makes the network more useful to everyone already inside it, and pulls the next buyer in.

Three weeks of evidence gathering becomes one afternoon.

DENSITY DRIVER · 5-15 COMPLIANCE-CRITICAL SUPPLIERS PER PROGRAMME



· REVENUE MODEL · PRICING ANCHORS Buyers route more work to suppliers who can answer quickly, so provability is upside, not only compliance.

Plan · 01 · Essentials

TIER-2 / TIER-3 MANUFACTURERS

€36K / CUSTOMER / YEAR

Compliance monitoring, multi-tier visibility, audit-ready evidence.

BLENDED ACV, €60K AT MATURITY · ANCHORED ON EXIGER, ASSENT, SIEVO BENCHMARKS

Plan · 02 · Enterprise

PRIMES & PROCUREMENT BODIES

€90K / CUSTOMER / YEAR

Agentic compliance, advanced analytics, air-gap deployment.

— FOUNDING TEAM

ENGINEERS WHO'VE BUILT AT **AMAZON SCALE.**

Eighteen years of engineering between them, now building the agentic evidence layer European defence needs.

**SUBHASISH DAS**

CO-FOUNDER · CTO

Engineering leader specialising in distributed systems and high-reliability backend architecture. Designed and scaled infrastructure for mission-critical services at Amazon, working alongside its global supply chain systems. Brings resilient systems, data pipelines and security-focused backend engineering.



LINKEDIN

X

SUBHASISH@SKANSAR.COM

**KALPESH SINGH**

CO-FOUNDER · CEO

Engineering leader with 10+ years building enterprise systems and the interfaces operators actually work in, alongside Amazon's global supply chain organisation. Led engineering teams across international environments. Owns commercial strategy and go-to-market.



LINKEDIN

X

KALPESH@SKANSAR.COM

— THE ASK

€2M · 18 MONTHS · FIRST PAYING CUSTOMERS.

€2M gives 18 months of runway, to 3–5 paying customers and ISO 27001 certification. EU defence investment reaches €163B in 2026, €547B of total spending projected by 2029. We are raising to be the agentic evidence layer already installed when that money has to be accounted for.

· MILESTONES

Month 03

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

Month 06

First paid deployment, Tier 2/3 manufacturer · pricing and onboarding model validated.

Month 12

2 paid deployments · 5+ manufacturers in active conversations · ISO 27001 audit started.

Month 18

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

· CAPITAL ALLOCATION

60%

PRODUCT & ENGINEERING

- AI document intelligence, automated classification across ITAR, EAR and EU Dual-Use.
- Agentic regulatory monitoring, autonomous agents propagating risk alerts in real time.
- Zero-trust architecture, buyer-scoped data isolation, encrypted audit trail.

20%

SECURITY & COMPLIANCE

- ISO 27001 certification, formal audit pathway for enterprise procurement.
- Penetration testing & red-team, independent validation of isolation & access controls.
- BSI C5 and AWS ESC, EU-recognised cloud security standards.

20%

GTM & DEPLOYMENTS

- Design-partner programme, 2–3 Tier-2/3 manufacturers in Germany & Benelux.
- Commercial & domain hires, first sales hire and a compliance specialist.
- Reference-customer programme, package the first deployment story for replication.

— · IF WE WIN

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

→ ONE THIN LAYER. SOVEREIGN BY DEFAULT.

Stripe became the rail for payments. Plaid for banking. Neither replaced the systems underneath. **DefenceOS** is the thin layer Europe's defence supply chain proves itself on, neutral, sovereign, audit-ready by default.

· BUILD IT WITH US

€2M first round

18 MONTHS · TO 3-5 PAYING CUSTOMERS

SUBHASISH DAS · CTO

subhasish@skansar.com

KALPESH SINGH · CEO

kalpesh@skansar.com

· WEB

skansar.com

MARKETING

app.skansar.com

LIVE PRODUCT

skansar.com/trust

SECURITY