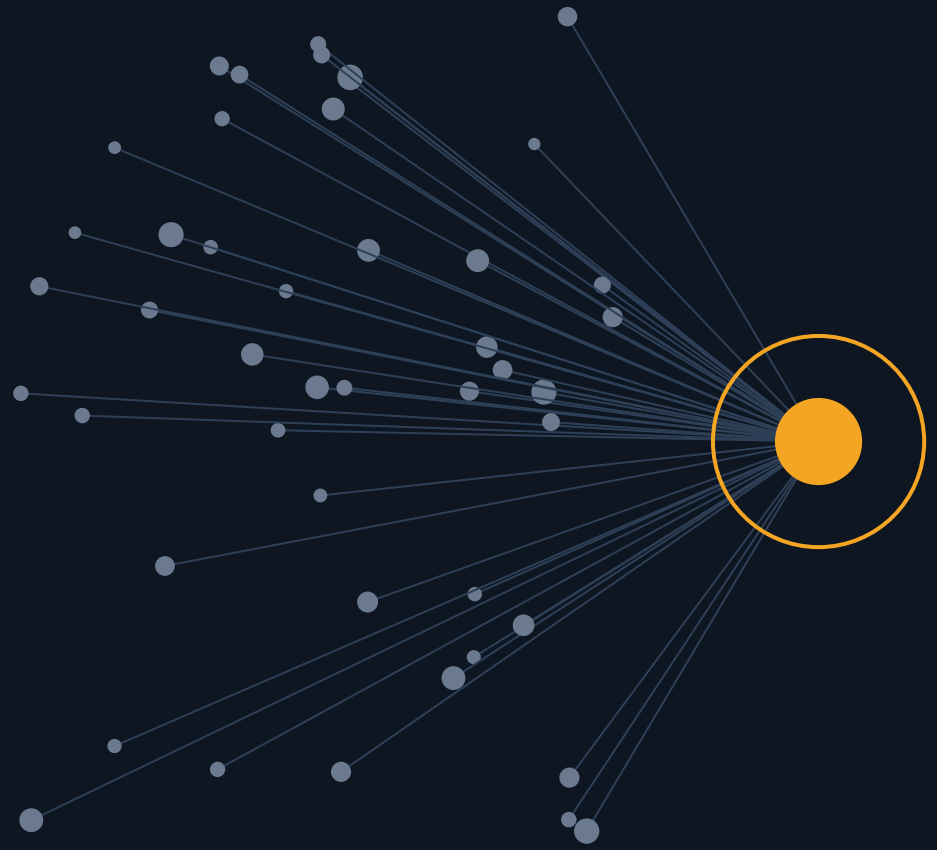
SemantIQ
powered by IKARUS

From signal to decision



Closing the gap between a threat signal and a proven action

The analysis layer for a Cyber Command and Control Center

Riegler Markus | Co-Founder | Cyber Threat Analyst | Riegler.m@ikarus-semantiq.at

THE QUESTION

Which threats affect us, when and where - and what options do we have against that?

SHORT TERM · TACTICAL

Which threats affect us today and tomorrow?

Today

The signals are spread over feeds, alerts and reports.
Exploited Vulnerabilities are analyzed by hand.

NEXT 30 TO 90 DAYS · OPERATIONAL

Which threats will affect us in the next 30 days?

Today

Campaigns and full operation descriptions are tracked by hand.
Reaction is too slow and binds too much resources.

90 TO 360 DAYS · STRATEGIC

Which threats must we prepare for in the future

Today

Trends are described in reports that nobody links to our own assets.

Today the answers come late, and we cannot prove how we reached them.

The signal to action gap



Fast

Feeds, sensors and alerts deliver signals in minutes.

Slow

People read reports, copy facts and check sources by hand.

Fast

Firewalls, EDR and playbooks act in seconds once an order exists.

Solution: We put the machine into the middle, and keep a person in command.

PROBLEM 1 · UNSTRUCTURED DATA

The signal is contained in unstructured data

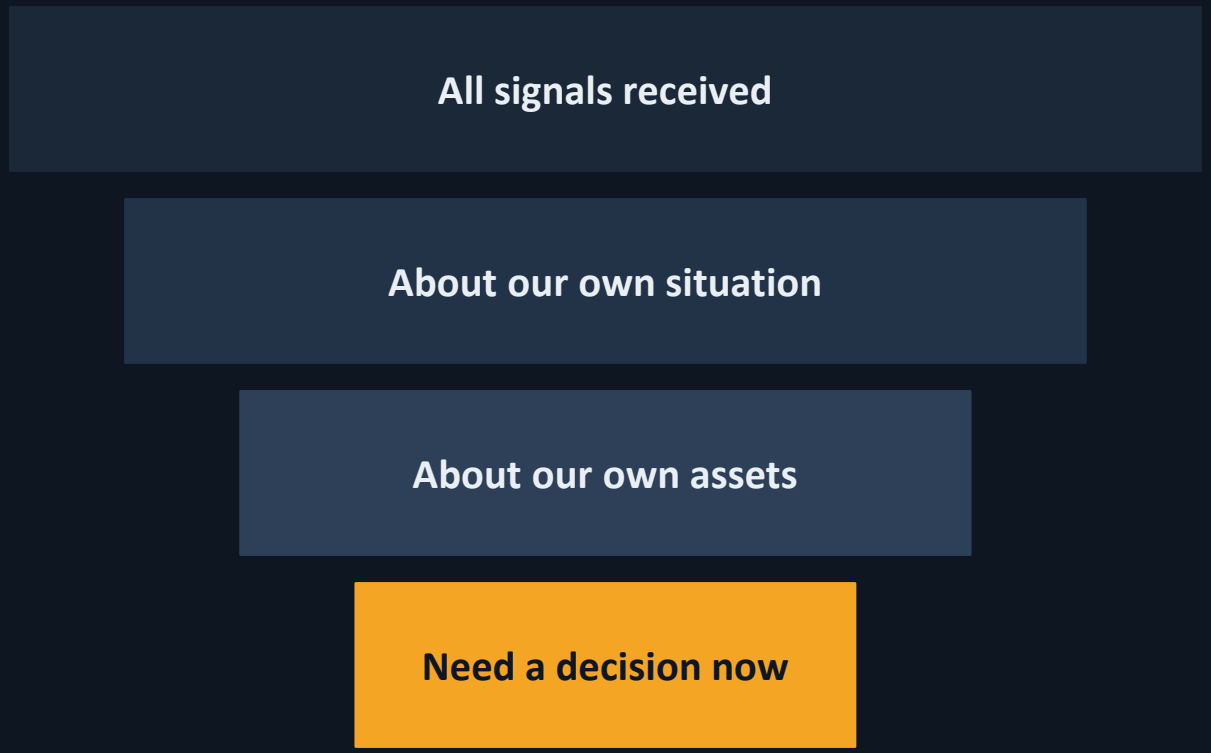
- PDF threat reports
- Vendor blogs and RSS
- CERT and NCSC advisories
- News and OSINT
- Images inside reports
- Partner and ISAC messages

Feeds deliver indicators. Reports deliver the meaning.

- Who acts, against whom, how and why now: this lives in unstructured date, not in structured feeds.
- Analysts read it and copy it out by hand.
- Indicators arrive without the story behind them (context).
- The Threat Information Platform fills information, not with understanding and knowledge.

PROBLEM 2 · SIGNAL QUALITY

Many signals, few that matter



Volume is not the problem. Selection is.

- An indicator without context is noise.
- Relevance depends on our assets and our intelligence requirements.
- Today the filter is a person reading by hand.
- Good signals are often missed. Weak signals are acted on.

PROBLEM 3 · EVIDENCE AND PROVENANCE

Before you act, you need proof

Question	Military	Cyber defence
Where	Target location	The affected asset or service
When	Time window	When it was seen, and whether it is still valid
With what	Weapon, means	Block, isolate, hunt, patch, warn, brief, etc.
On which evidence	Sensor, source	Source, document, how it was observed
On whose authority	Order, rules of engagement	The analyst decision and the release rules

No proof, no action. And after the action, we must be able to show why.

WHY TODAY'S TOOLS CANNOT GIVE THIS PROOF

Threat Information Platform - Three technical limits



An update deletes the old value

When the same source updates its own record, the previous value is replaced. Yesterday's state can no longer be seen.



Two sources are not compared

Different sources are stored side by side, or merged by a rule. The conflict itself is not held, source reliability is not weighted, and the analyst's decision is not stored.
No indication of contradicting information



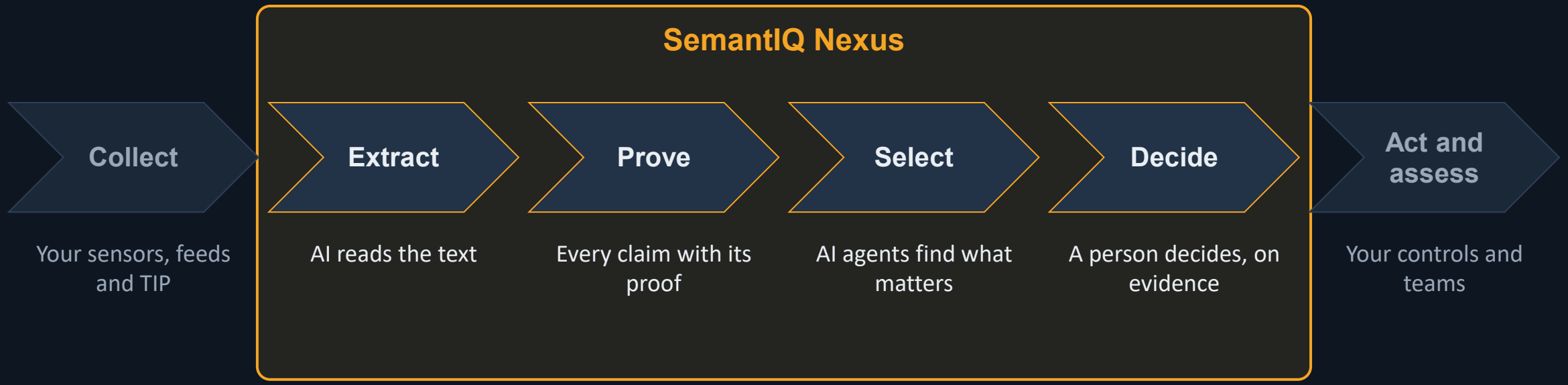
The analysis is not stored

Reports, notes and decisions live outside the system: in documents, mails and file shares.
No possible feedback channels back to the analysis.

A Threat Information Platform manages information. It does not produce intelligence.

FROM SIGNAL TO ACTION

SemantIQ Nexus - closes the gap in the middle

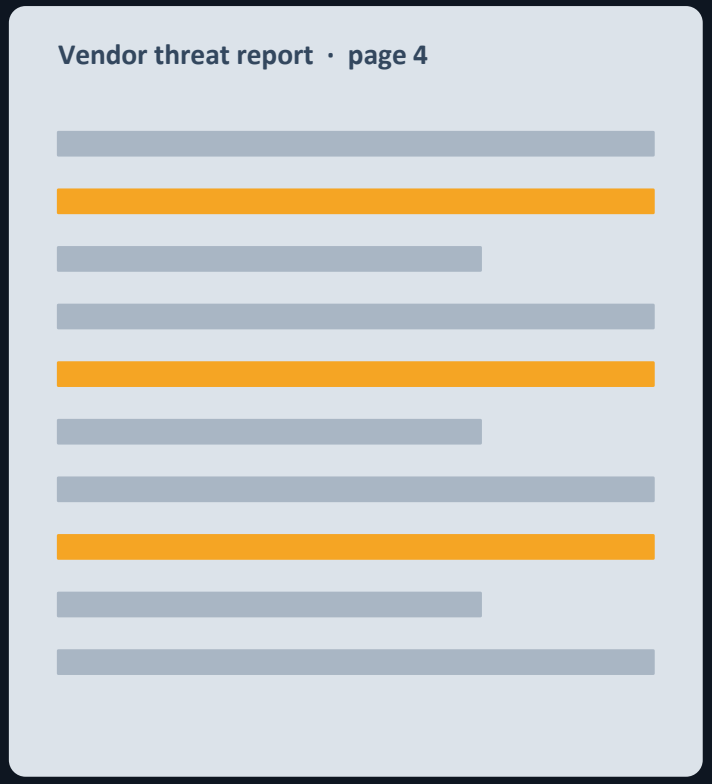


Your TIP and your tools stay.

Nexus is the intelligence cell of your Cyber C2 Center. It sits in front of the TIP as the analysis and production layer and returns intelligence products: back to the TIP and out to the stakeholder.

STEP 1 · EXTRACT

From unstructured data to claims – CTI Extraction



Campaign X → uses → spear-phishing (T1566)

Source: vendor report · p. 4 · line 12

Group X → targets → energy sector

Source: vendor report · p. 4 · line 21

Malware Y → uses → evil-cdn[.]example

Source: vendor report · p. 4 · table 2

- The AI CTI extractor reads PDF, web pages, RSS and images.
- It writes validated STIX 2.1 for graph modeling.
- Each claim points to its place in the source.
- The analyst reviews and accepts.

A claim is one statement from one source, with its date and its evidence.

STEP 2 · PROVE

Every claim carries its proof

Claim	**Group X uses spear-phishing against the energy sector**
Source	Vendor threat report
Recorded	When was the signal recognized
Valid	When it is true in the world
Confidence	How sure the source is
Evidence	How it was observed: p. 4, line 12



Old values are kept

Nothing is overwritten. You can see the state of any past day.



Conflicts stay visible

Two sources that disagree are both kept, side by side, with their proof.



Withdrawals are traced

When a source withdraws a report, every claim and product that used it is shown.

AI is a source like any other: its claims carry the same proof.

STEP 3 · SELECT

AI agents find the right signals based on Intel Requirements



New claims

- Which exploited vulnerabilities affect our software today?
- Which campaigns target our sector in the next 30 days?
- Which threats to our supply chain are rising according to ship transports?
- Which threats must we prepare for in 30 to 90 days?

The agent

checks new claims against our assets, drafts a short assessment and cites every source.

The analyst

accepts, corrects or rejects. The decision is stored as data.

The machine proposes, a person decides.

STEP 4 · DECIDE

Where, when, with what: answered with evidence



Situation report and decision support

Where	The affected asset or service in our own IT estate
When	The time horizon: today, next 30 days, 30 to 90 days
With what	Block, hunt, patch, warn a partner or ISAC, brief leadership
Why	The chain of claims and sources behind it
Who decided	The analyst decision, stored as data

Every action can be traced back to the signal that started it.

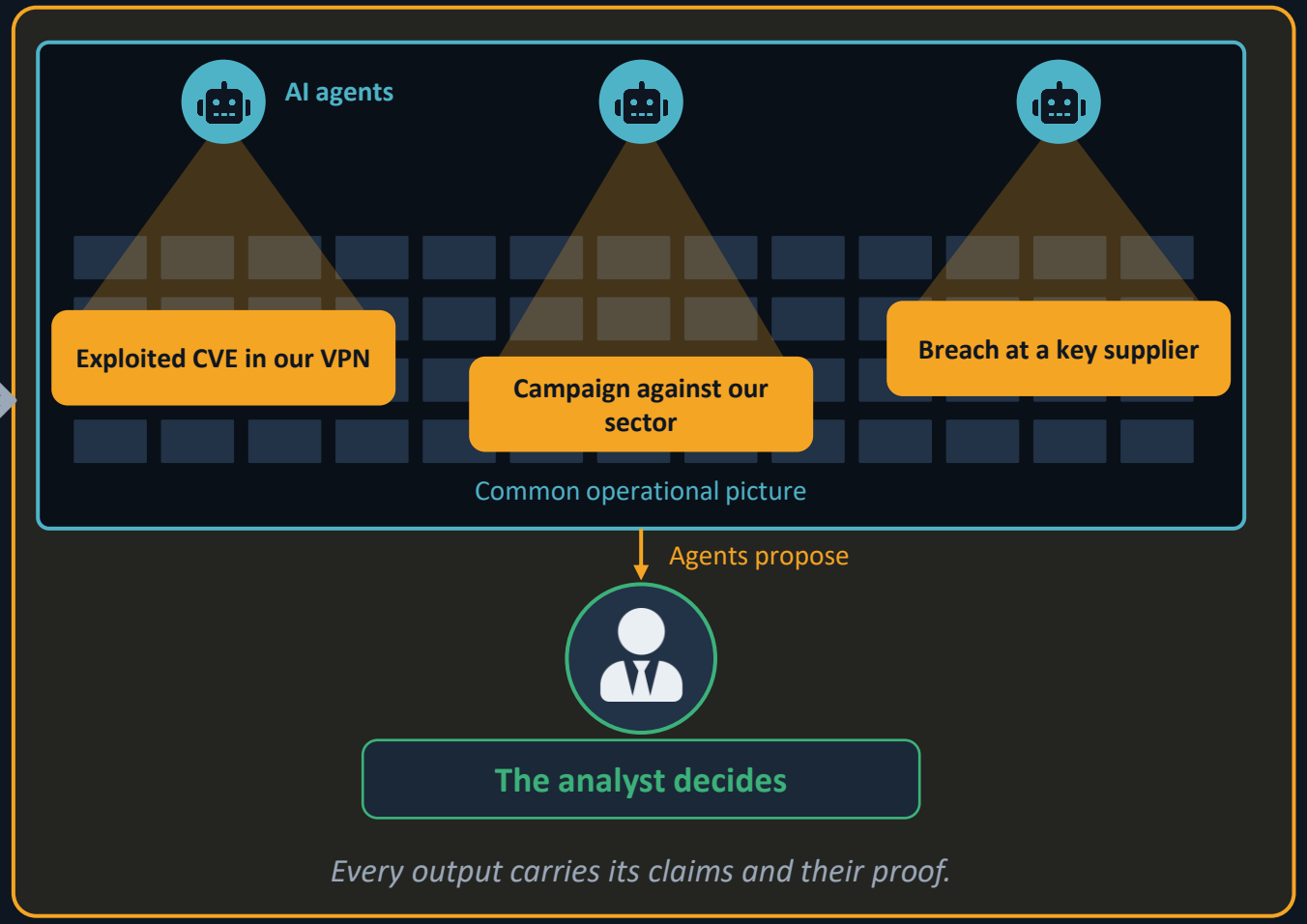
INSIDE THE CYBER COMMAND AND CONTROL CENTER

Agents and human's co-working space

Signals in

- Feeds and TIP
- Reports, Blogs, RSS and web pages
- Partner and ISAC
- Own telemetry and assets

Mostly unstructured: text, PDF, images

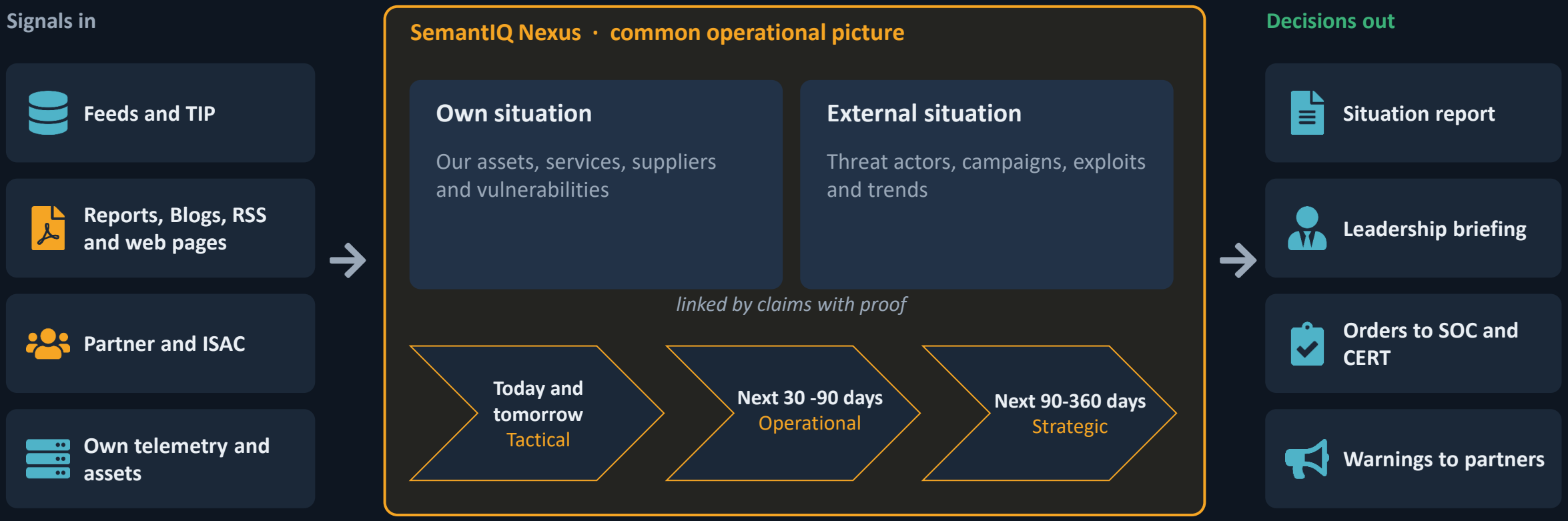


Decisions out

- Situation report
- Leadership briefing
- Orders to SOC (Hunt, Block, Detect, etc)
- Warnings to partners

THE CYBER COMMAND AND CONTROL CENTER

One picture, three time horizons



Every decision comes with its time horizon and its proof.

SOVEREIGN BY DESIGN

The data and the AI stay in your house

Your premises

- SemantIQ Nexus
- AI models, on-prem
- Your TIP
- Your analysts



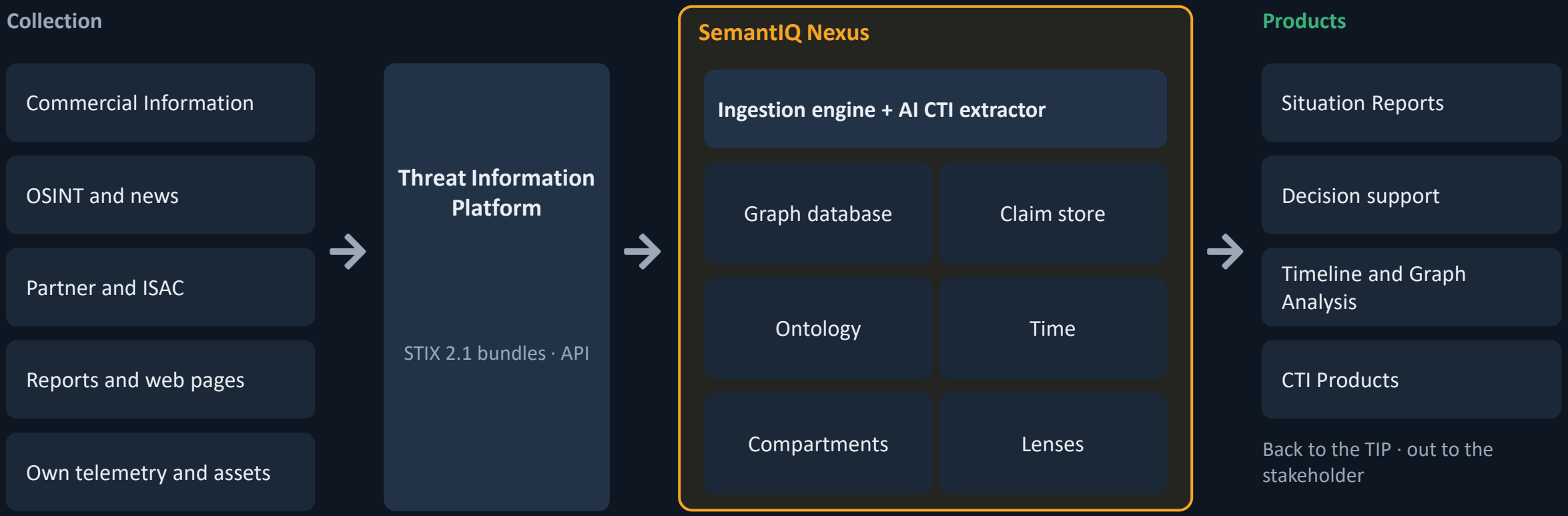
No external AI cloud needed

- On-prem and air-gapped operation
- AI in a box: models run on local hardware
- Several levels of secrecy in one system
- Developed in Austria for the European market

Sovereign Cybersecurity. Made in Europe.

HOW IT FITS

Reference architecture



From signal to decision. With proof.



Thank you

SemantIQ
powered by IKARUS

Riegler Markus | Co-Founder | Cyber Threat Analyst | Riegler.m@ikarus-semantiq.at