Your partner in the fight against (cyber)crime

DataExpert

DataExpert
YOUR PARTNER FOR 35 YEARS

Towards Sovereign AI Architectures for Complex Digital Investigations

Jacob Isaksen

Director,
Advanced Solutions

What we'll cover

DataExpert
YOUR PARTNER FOR 35 YEARS

What is the big deal?

What can be done?

Practitioner perspective from 10+ years of implementing secure digital forensics platforms at scale across government and enterprises

What is the big deal?

DataExpert
YOUR PARTNER FOR 35 YEARS

- AI as Investigative Infrastructure
- AI misconceptions
- Scale + Fragmentation Crisis
- Adversarial Acceleration
- External AI Dependency Risk
- The Monolith Problem
- The Trust Boundary Problem

AI as Investigative Infrastructure

DataExpert
YOUR PARTNER FOR 35 YEARS

AI is already becoming embedded across:

- Data ingestion
- Translation (machine ↔ human)
- Summarisation and reporting
- Analytical workflows

= AI is becoming part of the investigative substrate

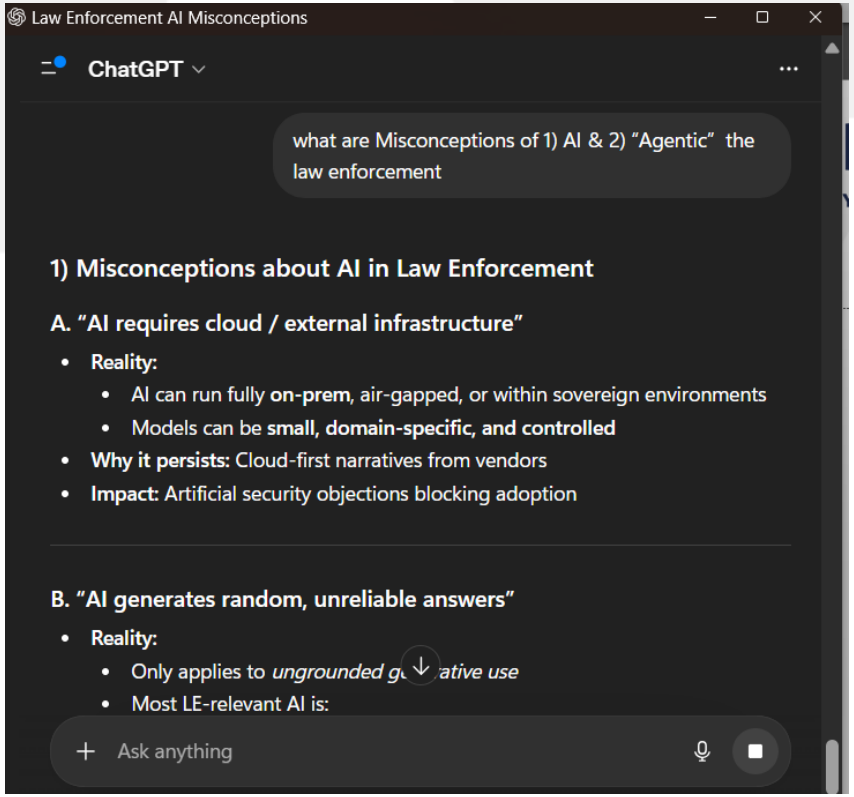
- The role of AI should be:
  - Transformation and interpretation
  - Not evidential authority

…But is at risk of being used and perceived differently

Misconceptions: AI & “Agentic” in LE

DataExpert
YOUR PARTNER FOR 35 YEARS

- **Assumption**
  - AI = cloud and huge frontier models
  - AI = Generative random answers
  - Agentic = autonomous LLMs
- **Consequence**
  - “AI cannot use AI due to security reasons”
  - “We risk putting the wrong people in jail”
  - Prolific use of *Shadow AI*



Scale + Fragmentation Crisis

DataExpert
YOUR PARTNER FOR 35 YEARS

- Investigations now involve:
  - Multi-domain, multi-format data
  - E.g. unstructured, structured, sensor data, feeds, etc.
  - Ever increasing legal complexity
- Tooling:
  - Broad set of valuable tools
  - Specialised but disconnected

- **Result:**
  - **Manual stitching of workflows**
  - **Loss of context and tempo**
  - **Backlogs**

Adversarial Acceleration

DataExpert
YOUR PARTNER FOR 35 YEARS

- Criminals use AI:
  - Automated fraud
  - Identity fabrication
  - Scalable deception, and much more…
- Accelerated by:
  - Vibe-coding, serverless, agentic automation, open source scripts, etc.
  - Ie. adversaries operate as integrated AI systems

Key question:

- **Should we embrace scalable patterns used by adversaries?**

External AI Dependency Risk

DataExpert
YOUR PARTNER FOR 35 YEARS

When trying to do embrace adversarial AI capabilities…

- Reliance on external AI services:
  - API-based access (OpenAI, Anthropic, Microsoft Copilot, etc.)
  - Foreign infrastructure risk
  - Vendor-controlled execution

- Risks:
  - Data leaves investigative boundary
  - Unclear vendor monitoring / logging / debugging layers exist
  - Limited transparency on access and handling

Control over AI processing becomes decoupled from investigative control

The Monolith Problem

DataExpert
YOUR PARTNER FOR 35 YEARS

Emergence of **large, integrated intelligence platforms**

- Common narrative:
  - “We need close and locked-in partnerships with only the best vendor(s)”
  - “No one else can do what they can”
- Reality:
  - These systems are:
    - Compositions of standard components
    - Wrapped in tightly coupled architectures
- Risks:
  - Vendor lock-in
  - Limited portability
  - Difficult to integrate best of breed

Monolithic systems centralise capability - but also centralise control with the vendor

The Trust Boundary Problem

DataExpert
YOUR PARTNER FOR 35 YEARS

- Common law enforcement and intelligence scenario:
  - **limited AI use today**
  - Primarily embedded in:
    - existing software platforms
    - small-scale LLM pilots / PoCs

- However, AI adoption is accelerating through:
  - Hidden inside tools
  - Ad hoc experimentation
  - Shadow AI

- As AI becomes embedded:
  - Processing may occur:
    - inside vendor-controlled components
    - or external infrastructure layers

- Your visibility into…
  - execution
  - data handling
  - model behaviour

  …becomes limited

Conclusion: The trust boundary is beginning to shift - before it is fully understood or deliberately designed

The big deal? In conclusion.
The risk of how will AI be introduced

DataExpert
YOUR PARTNER FOR 35 YEARS

Risk trajectory:

- fragmented control
- unclear data flows
- architectural lock-in

Required shift:

- Move from vendor-controlled AI adoption → to **sovereign architected AI integration**

Objective:

- Ensure AI is introduced within systems that are:
  - Controlled
  - Auditable
  - Designed for sovereignty from the outset

Transition:

- The need for **sovereign AI architectures as a design principle**

The issue is not that agencies are already dependent on AI.

It's that they are about to become dependent, but unintentionally.

DataExpert
YOUR PARTNER FOR 35 YEARS

What can be done?

What can be done?

- **Defining Sovereign AI Architectures**
- **Getting it right: Perception of AI**
- **Sovereignty vs Monoliths**
- **Reference Architectures**
- **Example: Agentic + Controlled Workflows**
- **Operational Requirements**

DataExpert
YOUR PARTNER FOR 35 YEARS

Defining Sovereign AI Architectures

- Systems where institutions retain control over:
  - Data
  - Models
  - Execution environments
- Key characteristics:
  - Modular
  - Interoperable
  - Replaceable components
  - Auditable by design

Anchor:
Open, sovereign architecture principles

Getting it right: Perception of AI

DataExpert
YOUR PARTNER FOR 35 YEARS

- **Assumption**
  - AI = cloud and huge frontier models
  - AI = Generative random answers
  - Agentic = autonomous LLMs
- **Consequence**
  - “AI is not allowed here
  - “We risk putting the wrong people in jail”
  - Shadow AI

- **Reality**
  - Open-source/weight models
  - Runs on-prem / private infrastructure w. GPUs
  - Proper use cases (extraction, summaries, syntax, computer vision, etc.)
  - Human in the loop
- **Agentic AI systems**
  - More about workflows + scripts
  - Deterministic pipelines and search
  - LLM = small component
- **Implication**
  - No dependency on cloud
  - No need for frontier models
  - Fully controllable systems

(hoping for more chipmaker diversity)

Sovereignty vs Monoliths

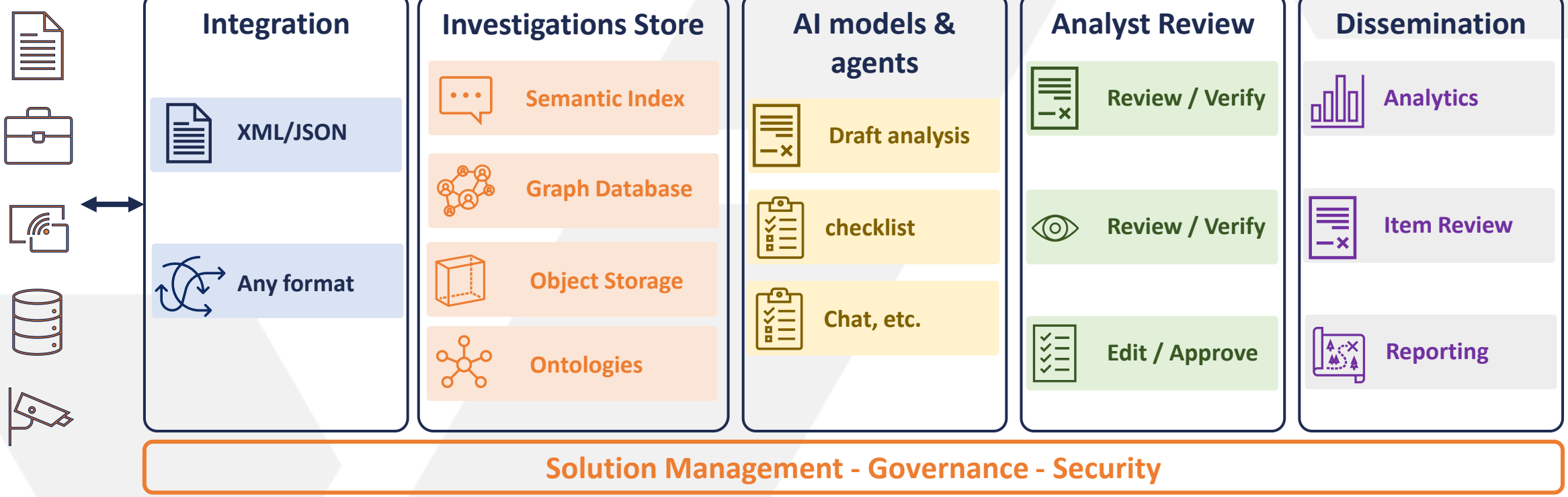
DataExpert
YOUR PARTNER FOR 35 YEARS

Monolithic Platforms	Sovereign Architectures
Vendor-controlled stack	Institution-controlled stack
Tight coupling	Modular components
Limited portability	Replaceable components
Opaque processing	Auditable pipelines
Strategic dependency	Strategic optionality

Sovereignty is achieved through **architecture, not vendor selection**

Reference Architectures

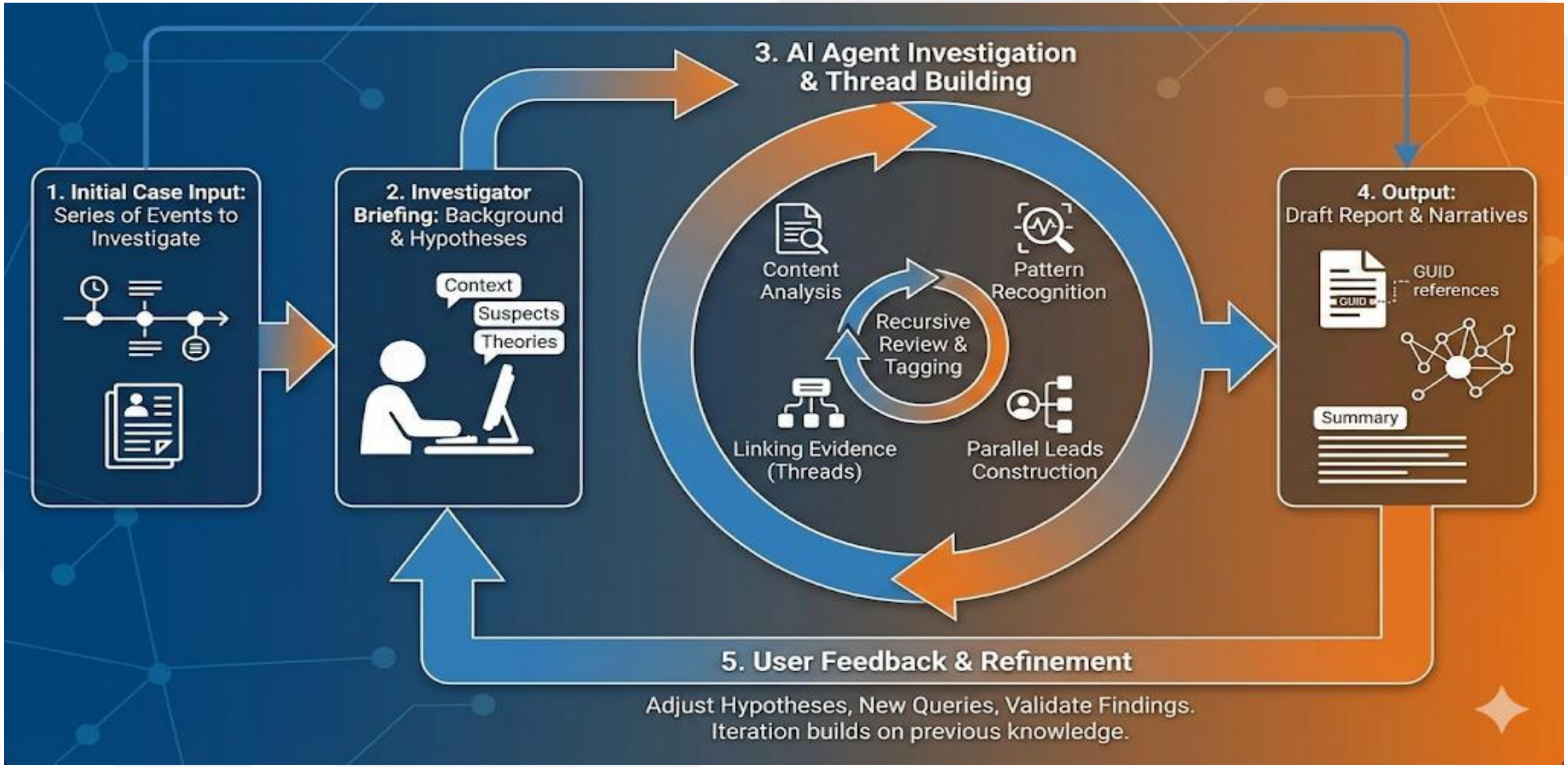
DataExpert
YOUR PARTNER FOR 35 YEARS



Digital Forensics | Data Analytics | Cyber Security | OSINT | Academy | Investigation

Example: Agentic + Controlled Workflows

DataExpert
YOUR PARTNER FOR 35 YEARS



Operational Requirements

DataExpert
YOUR PARTNER FOR 35 YEARS

Non-negotiable:

- Audit trails
- Data provenance
- Explainability
- Reproducibility

- Alignment:
  - ISO 17025, ISO9600, ISO2700x
  - EU regulatory frameworks

In summary

DataExpert
YOUR PARTNER FOR 35 YEARS

- Investigations are becoming **architectural challenges**
- AI introduces **new trust boundary risks**
- Monolithic platforms introduce **strategic dependency**

- **Sovereign AI architectures** enable:
  - **Control**
  - **Transparency**
  - **Long-term adaptability**

Questions?

DataExpert
YOUR PARTNER FOR 35 YEARS

Jacob Isaksen
Jacob@dataexpert.dk
+45 53500294