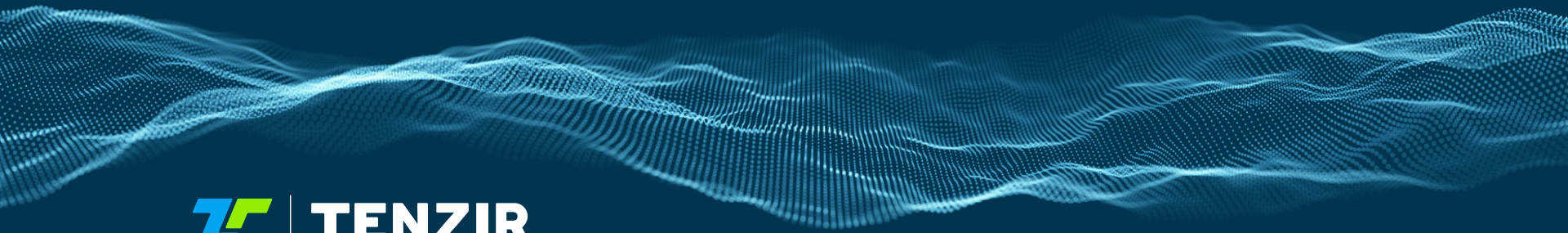
Security Data Engineering

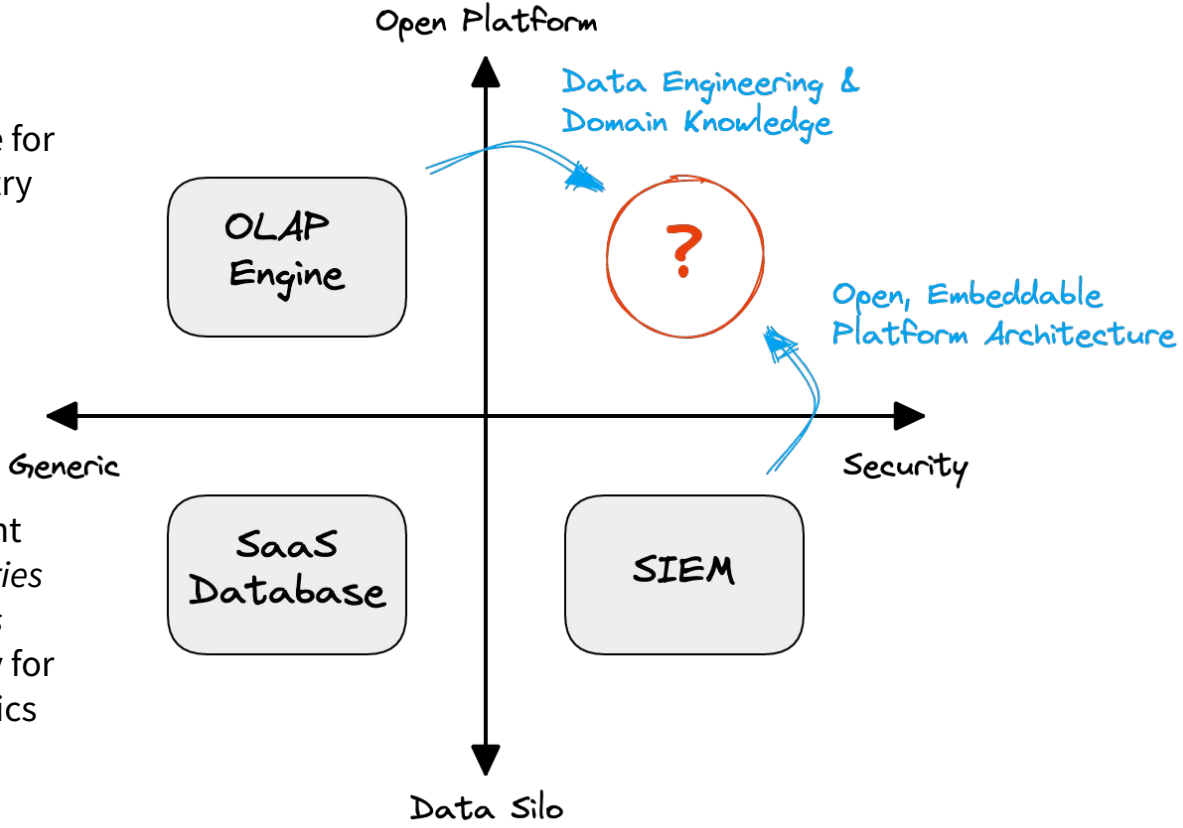
Matthias Vallentin, PhD



TENZIR

What is VAST?

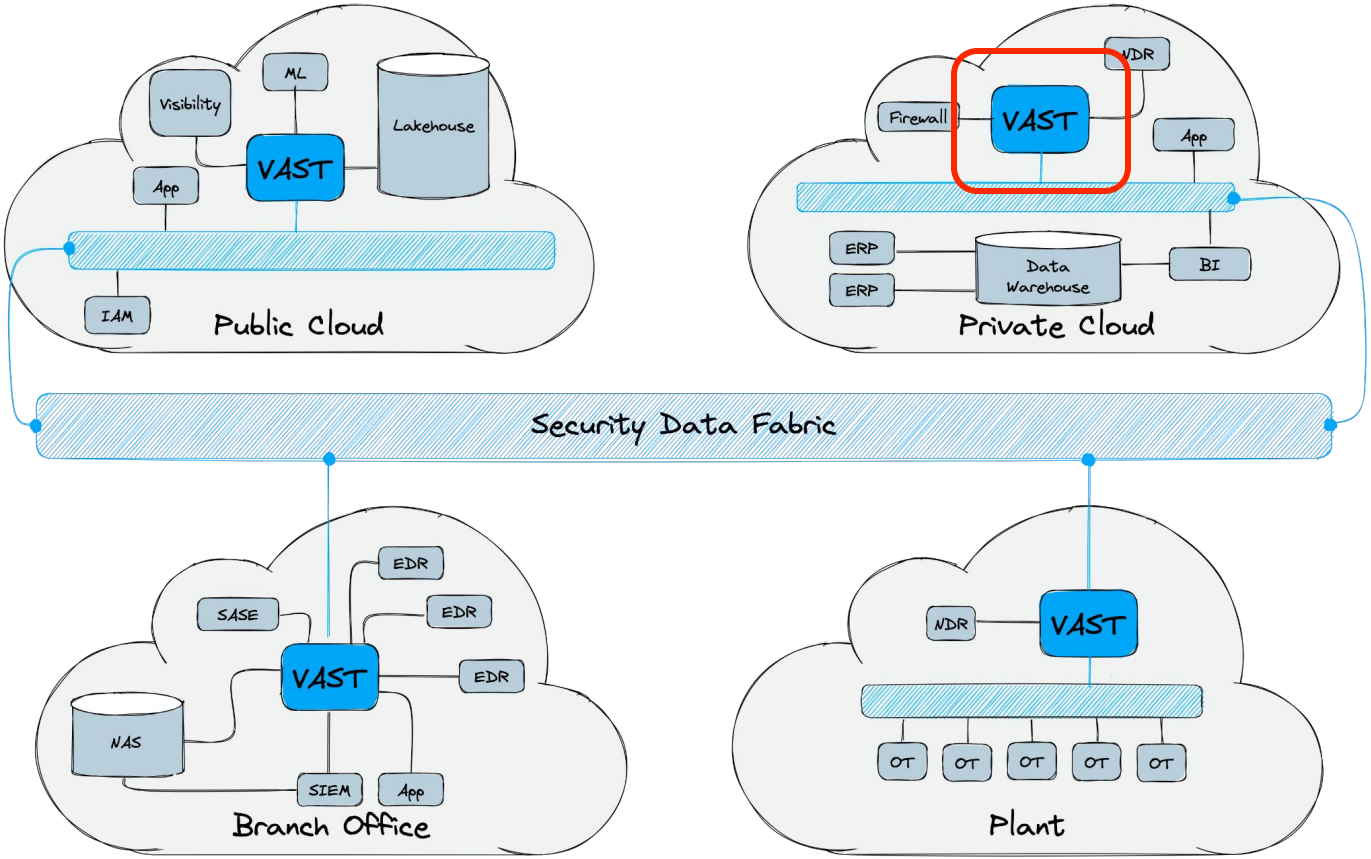
VAST: An embeddable engine for high-volume security telemetry and security operations



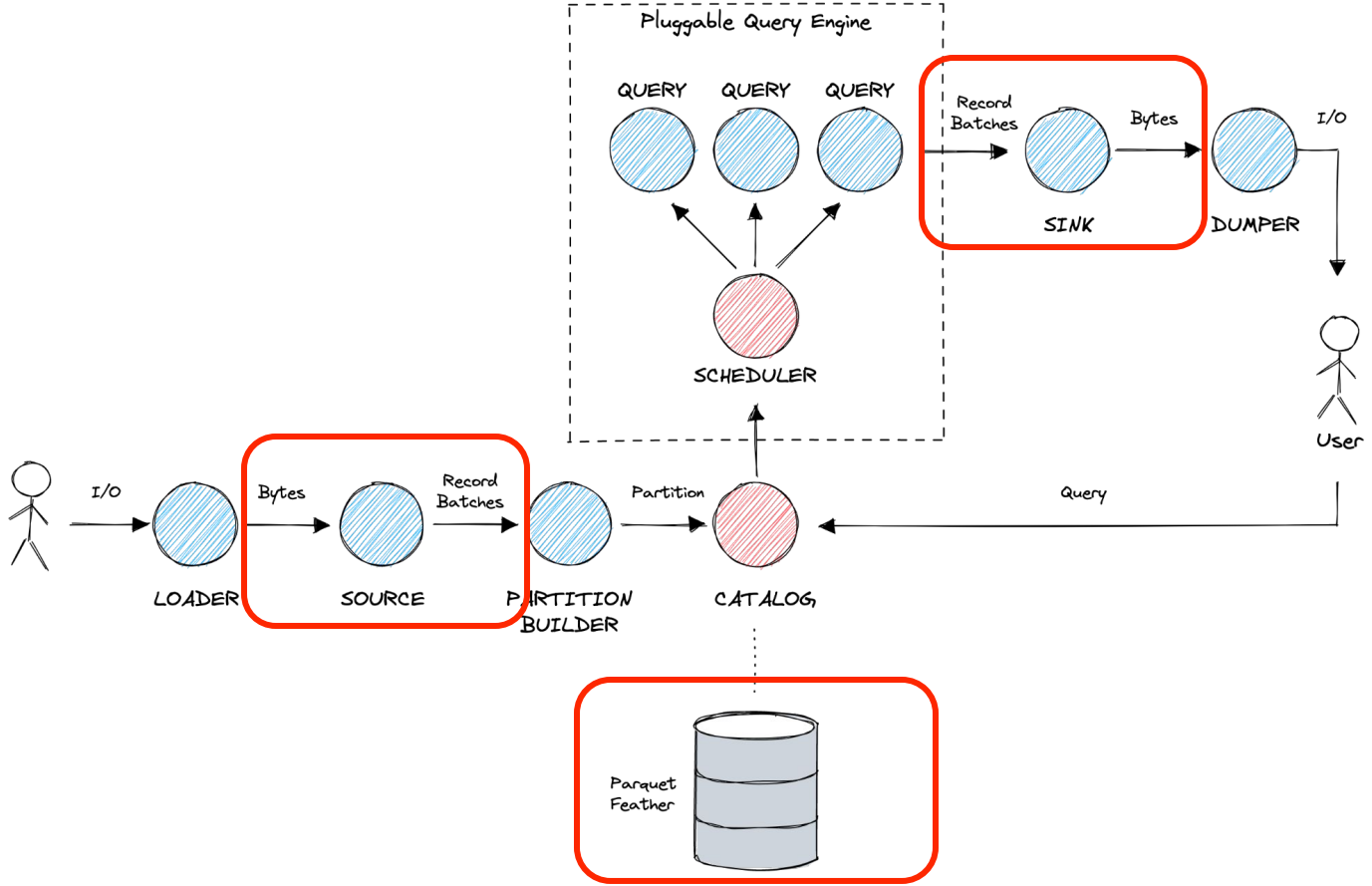
Data-centric Use Cases:

- Execute security content
  → *automated retro queries*
  → *in-stream/live queries*
- Record security activity for compliance and forensics
  → *write-path-heavy DB*

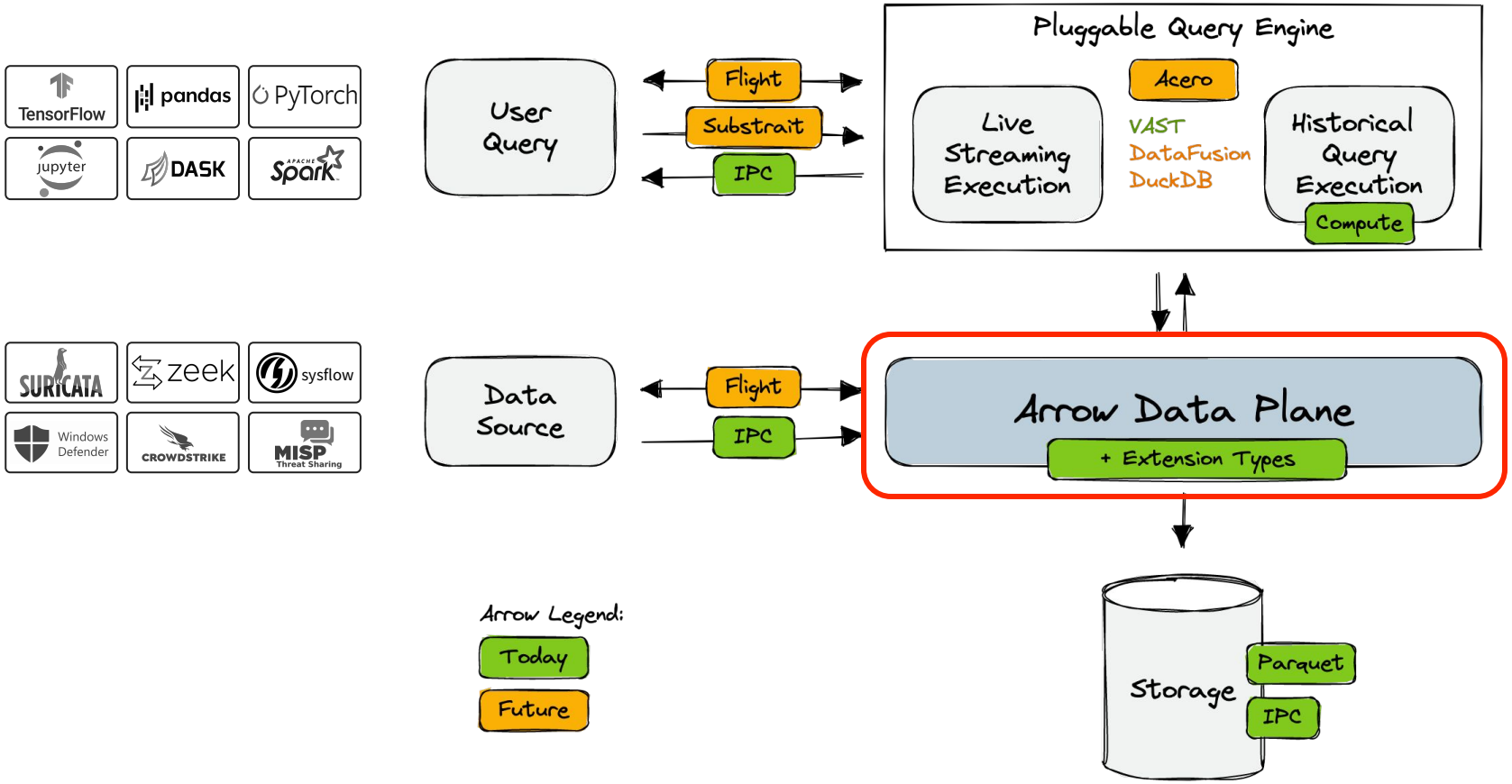
VAST Deployment Concept



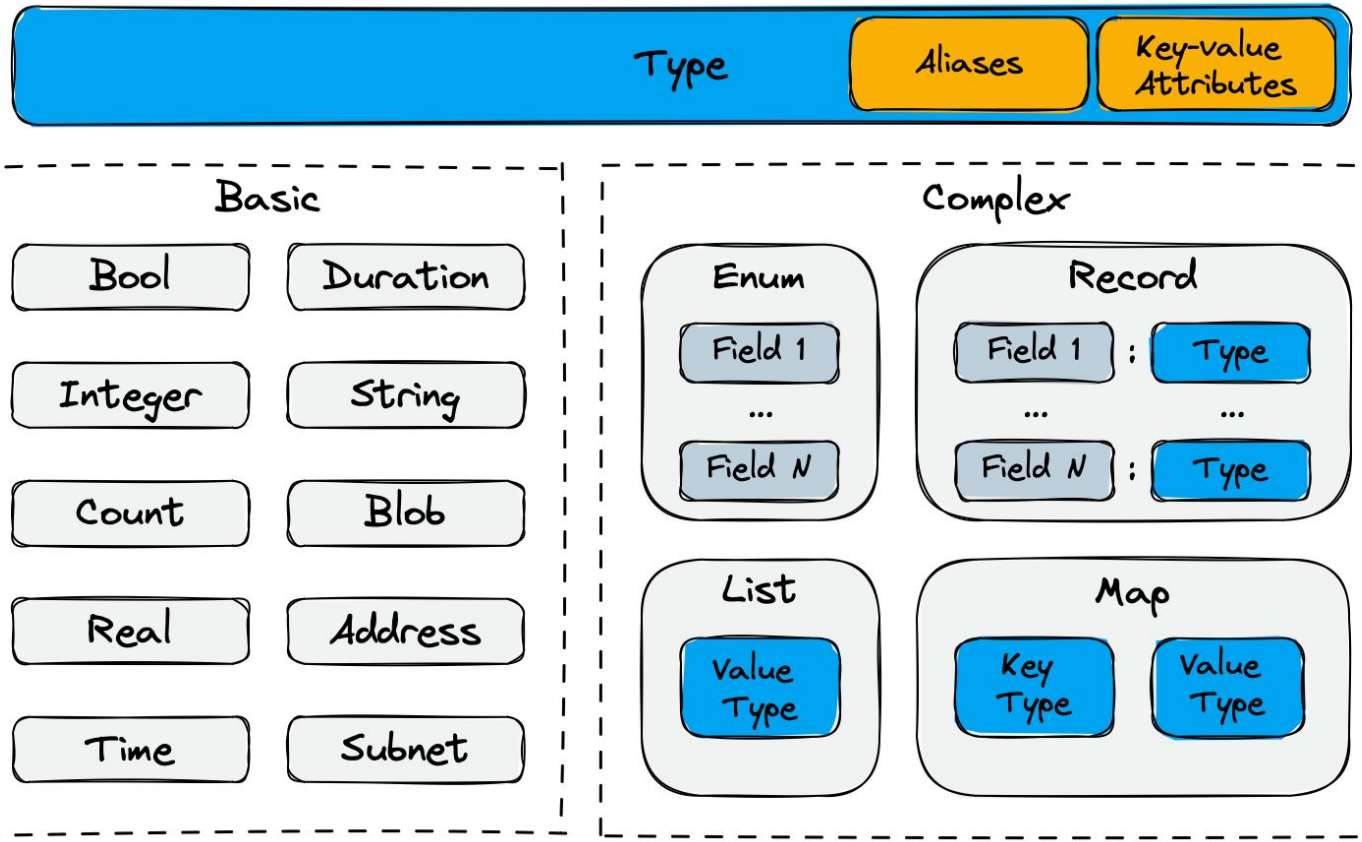
VAST Architecture



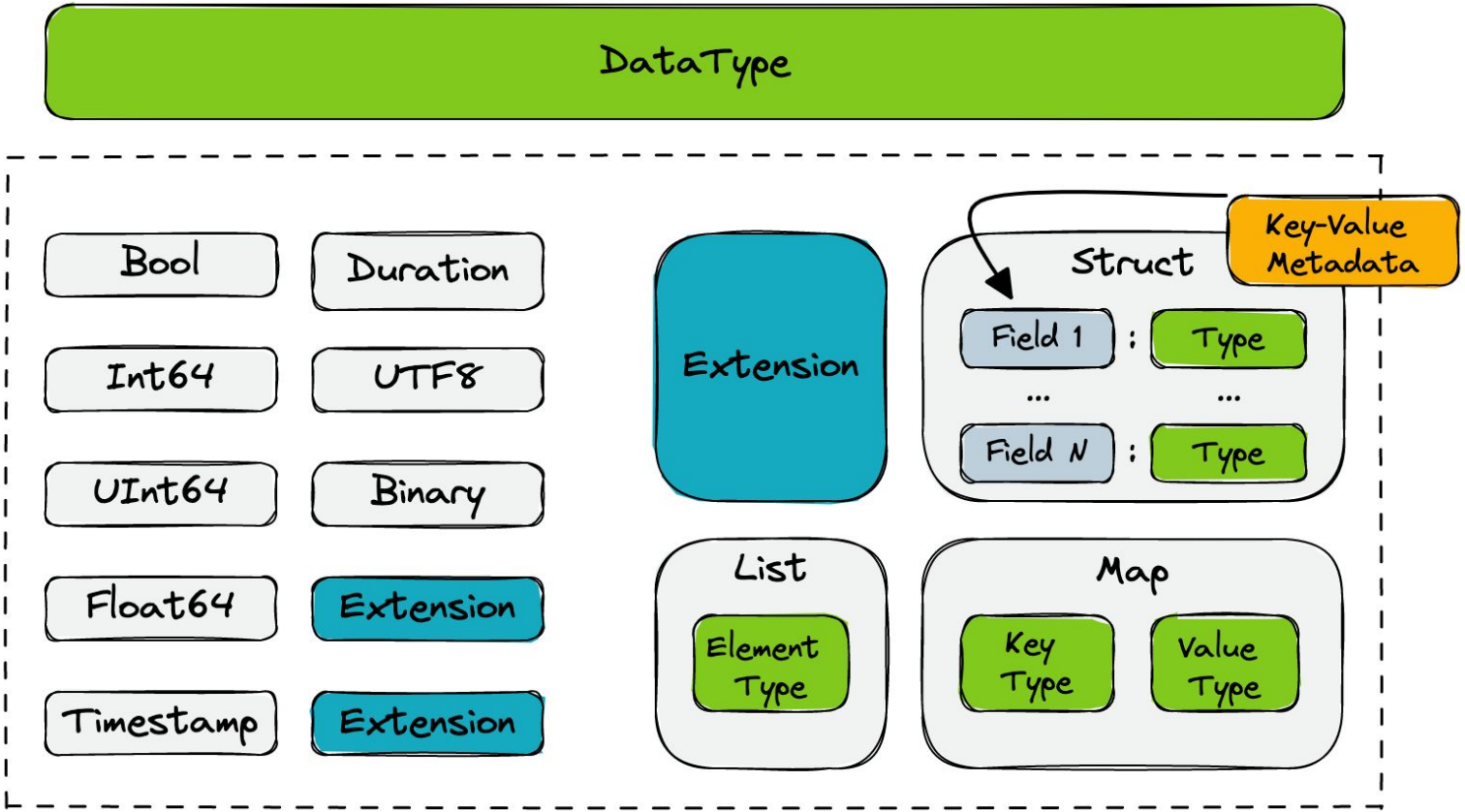
Arrow Data Plane and Engine



Rich-Typed Data Model



Arrow-compatible Type System



Summary

- **VAST**: embeddable engine for processing high-volume security telemetry
- **Arrow**: key enabler for security analytics
  - Bridges ecosystems via data interoperability
  - Provides standardized framework for heavy data lifting
    - In-memory: RecordBatch, Table
    - Persistence: Parquet, Feather
    - Versioning: FlatBuffers

➢ An open platform for data-first detection and response

https://vast.io

Join our Community Slack!

http://slack.tenzir.com

👉 https://vast.io/blog/apache-arrow-as-platform-for-security-data-engineering