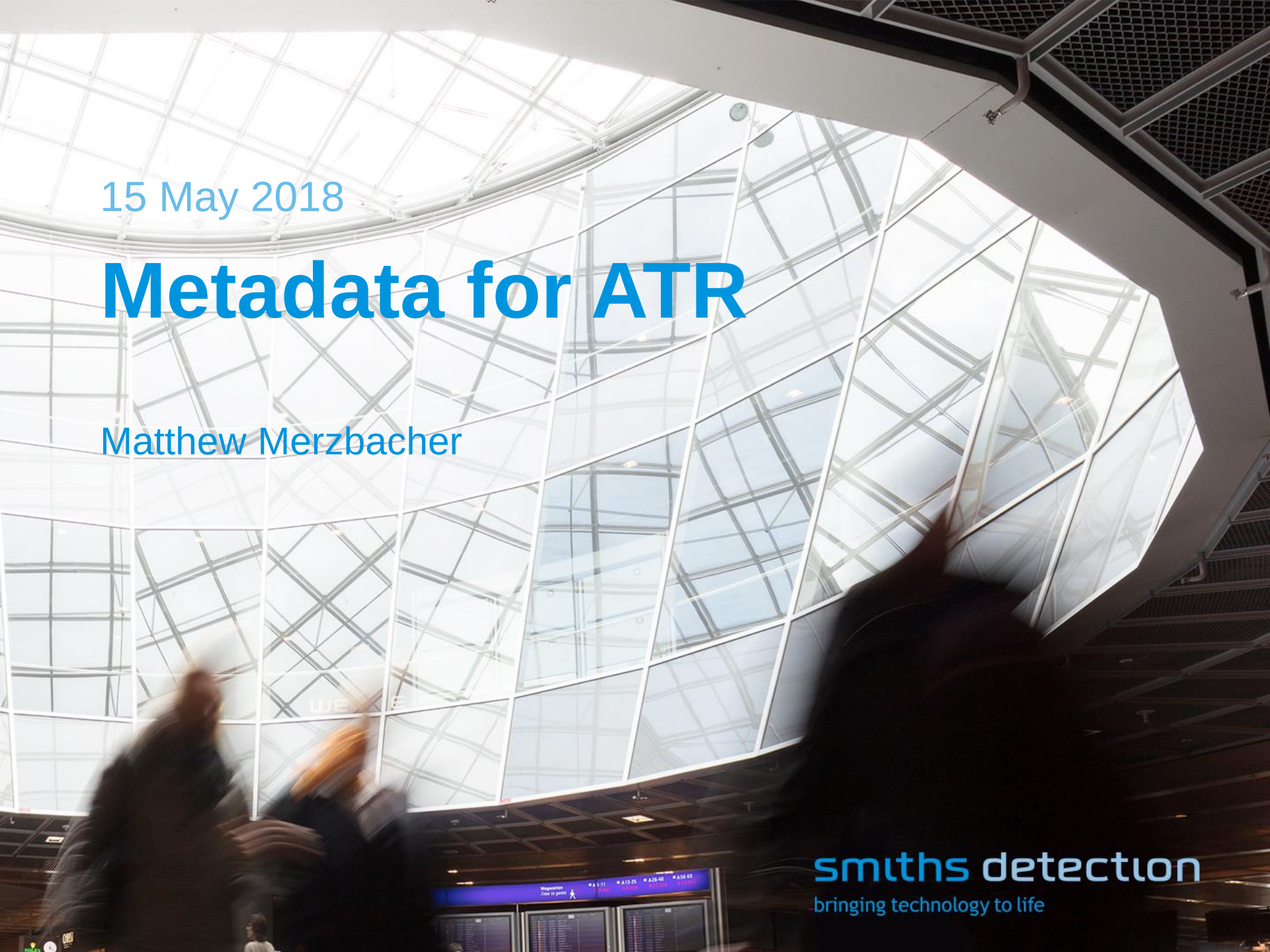


15 May 2018

Metadata for ATR

Matthew Merzbacher

smiths detection

bringing technology to life

Overview

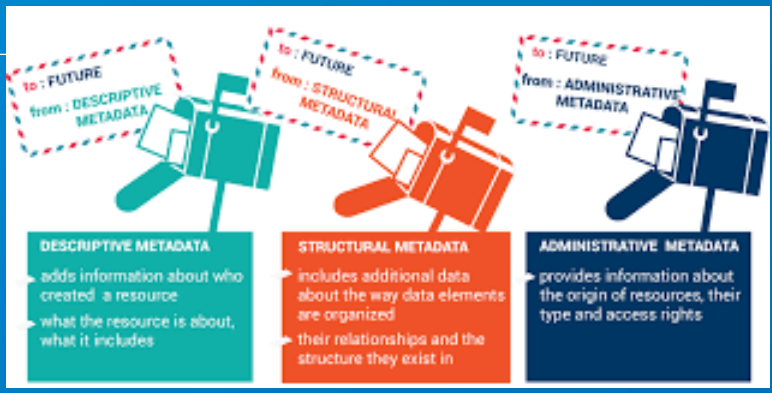
- Terminological Minute: Metadata vs. Abstraction
- Do we need Metadata?
- Metadata and Reduction
- A Few Uses
- Problems
- Will using Metadata work for security applications?

(Why) Do we Need Data Meta-Data in Security?

- Everything is going fine... Isn't it?

- Fundamental Formula for Security
  - Effort = (Volume * Det_Reqs * Size) / Screening_Speed
- Volume (number of passengers, bags, etc.) is increasing
- Detection Requirements continue to spiral
- Screening Speeds are not keeping up
- The only knob left is Problem Size
  - Use of abstraction / meta-data is a qualitative opportunity to reduce the size of the problem

One kind of Abstraction: Metadata



- Metadata is Data about Data
  - Descriptive (“what is the data”)
  - Structural (“how is it laid out”)
  - Administrative (“when/where/who”)
- Example: Telephone
  - Data (Content): Conversations
  - Metadata Abstraction: Records indicating participants, time & length of conversations
  - Easier to analyze call records than every conversation
    - Much less data with (almost) equal richness

- Is who/when/where we are screening as important as what?

smiths detection

Another kind of Abstraction: Reduction

- Rely on a previously solved problem or reduced problem
- Some Security Examples
  - Anomaly detection
  - Random selection
  - TSA Pre✓®
  - Dynamic Switching
  - Threat levels
  - Clear Bag / Benign identification

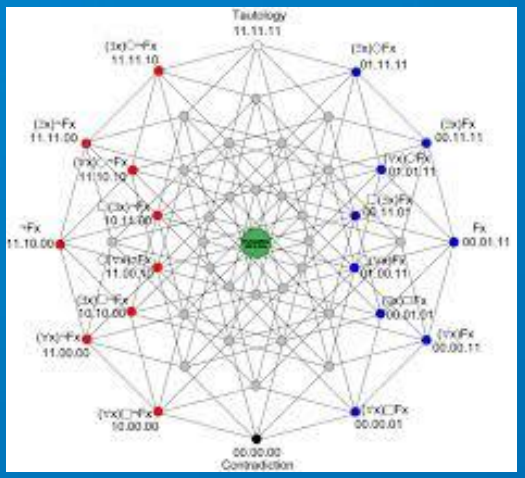
- Is who/when/where we are screening as important as what?

Some Potential Uses of Metadata in Security

- 1:1 – Did today's scan of Carl (or his stuff) look like prior scans?
  - Requires: Passenger ID verification, Representation of last week's scan, Trust in last week's scan
  - Will this allow us to scan him more quickly?
- 1:N – Does this look like a legitimate business/vacation traveler?
  - Requires: Manifest
  - How do we validate? Will Deep Learning help?
  - What happens as things change over time?
- Does combining carry-on and AIT results offer additional information?
  - Requires: Data Representation, Logic for combining, Ability to coordinate and combine correctly
- How could (probably classified) intelligence information inform the decision process?
  - Requires: Knowledge representation, control

Problem: Language and Logic of Abstraction

- Need a logic and method to use that logic
  - Distinguish data from information from knowledge
  - Describe system
  - Analyze performance & gaps
  - Describe change to data and change to world
- Knowns and Unknowns
  - X is true
  - X is false
  - The truth of X is unknown to me
  - I didn't even know X was an option



Additional Challenges / Closing Thoughts

- How do we resolutely protect/enhance civil liberties in a world of Metadata?

- Will using Metadata work for security applications?
  - Can we define the threat space or, at least, part of the benign space (for clearing)?
  - How do we evolve as conditions change?
  - Are we in an open or closed world?
    - How do we identify radicalization?

- When will the use of Metadata fail and how spectacularly?