
17 October 2018
AATR: Vendor's Response
Matthew Merzbacher
smiths detection
bringing technology to life

Who Voted you King?

- Problem: Fielding a response to an emerging threat is slow
- Goal: Same-day deployment of solutions

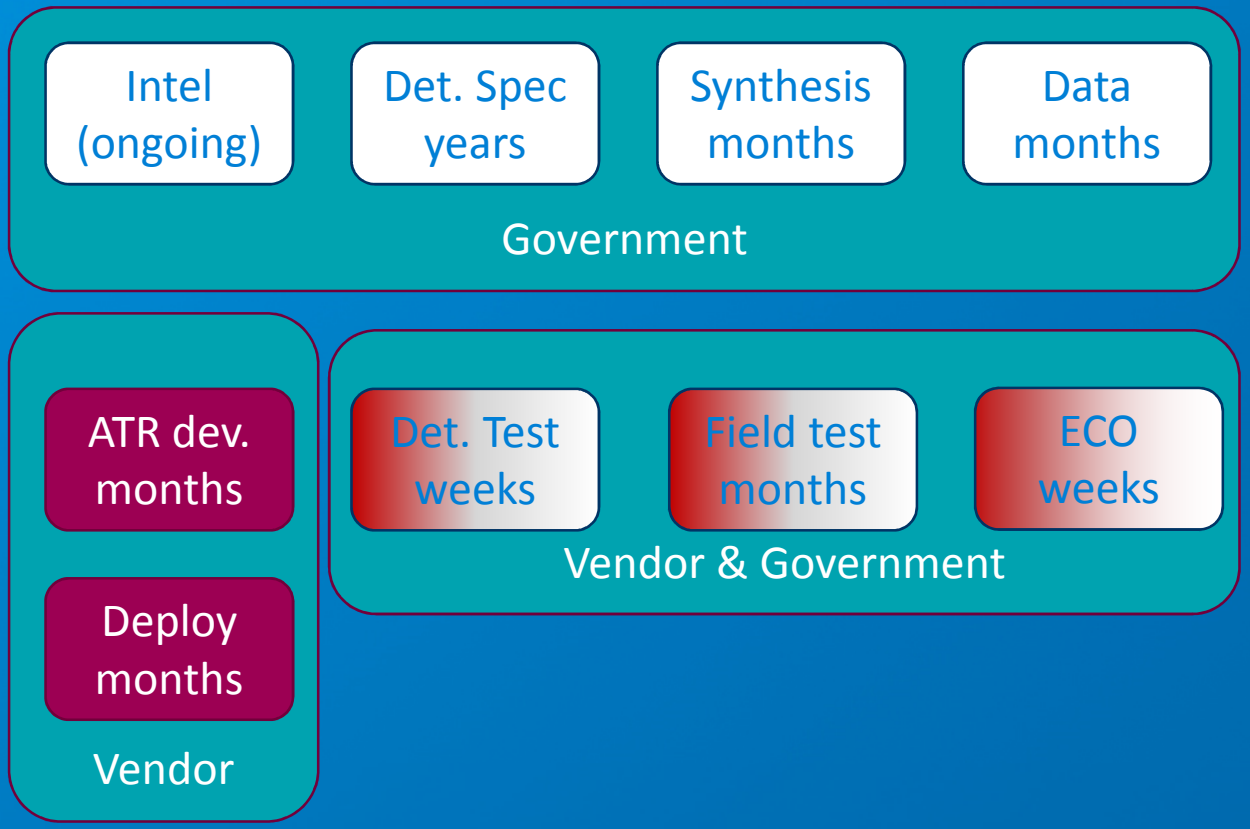
- The current process fails in that goal
  - Today: new threat means accept (for a long time) or shut-down

- How can we accelerate… and at what risk?
  - Take the modern “service” approach: field first, ask questions later
  - Does the approach make sense?
  - What else makes sense?
  - Where are the gorillas?
    - Hint: they aren’t where you think they are!

Current Process

- Serial
- Risk-Averse
- Lengthy

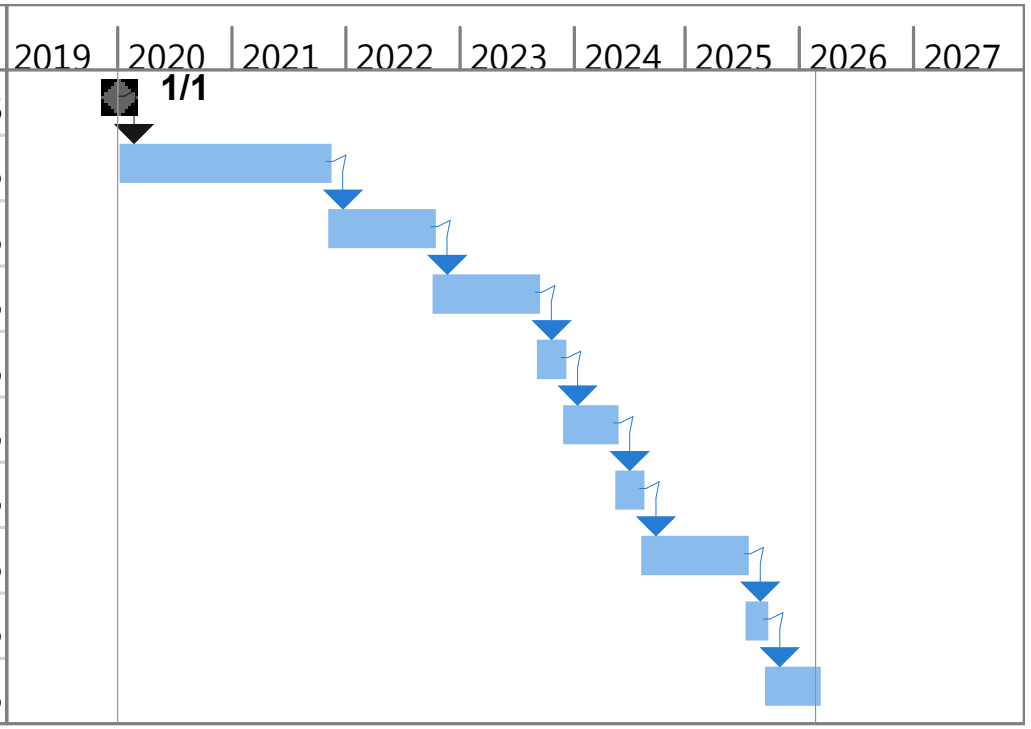
- Can be accelerated… some



In Gantt Form

- Almost realistic

ID	Task Name	Duration
1	Intel	0 days
2	Write Spec	24 mons
3	Synthesize Threa	12 mons
4	Collect Data	12 mons
5	Provide Data	3 mons
6	Develop ATR	6 mons
7	Test Detection	3 mons
8	Test for Field	12 mons
9	ECO	2 mons
10	Deploy	6 mons

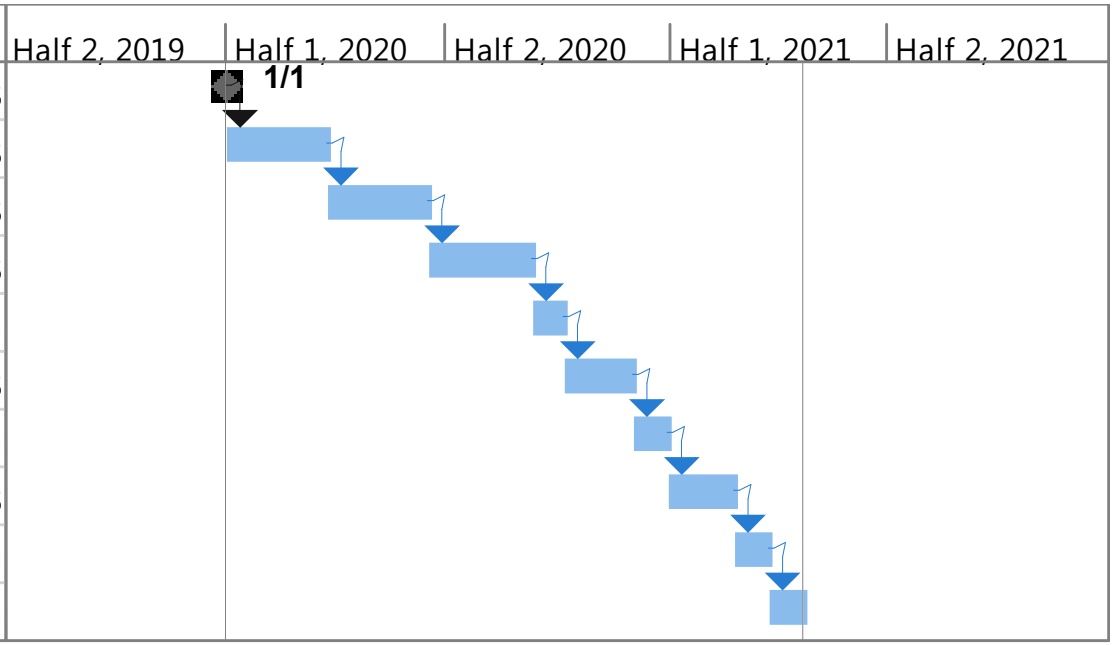


- By the time deployment happens, intel has identified a new threat
- What if we try to go faster?

Accelerated

- Optimistic

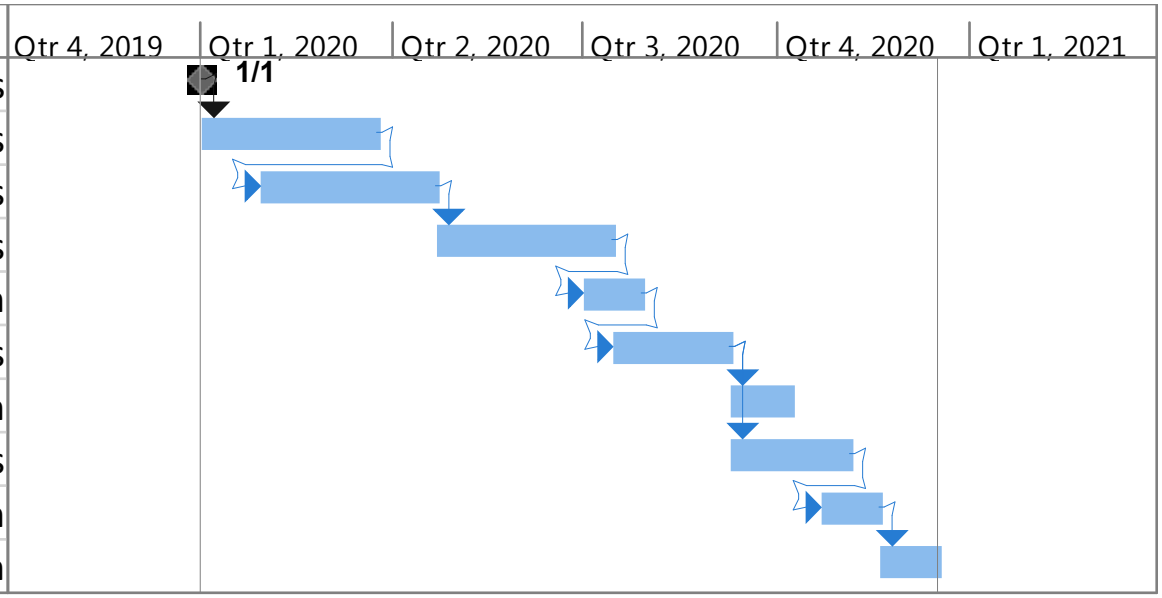
ID	Task Name	Duration
1	Intel	0 days
2	Write Spec	3 mons
3	Synthesize Threa	3 mons
4	Collect Data	3 mons
5	Provide Data	1 mon
6	Develop ATR	2 mons
7	Test Detection	1 mon
8	Test for Field	2 mons
9	ECO	1 mon
10	Deploy	1 mon



- Requires some risk acceptance
- Still suffers from serialization

Parallelized

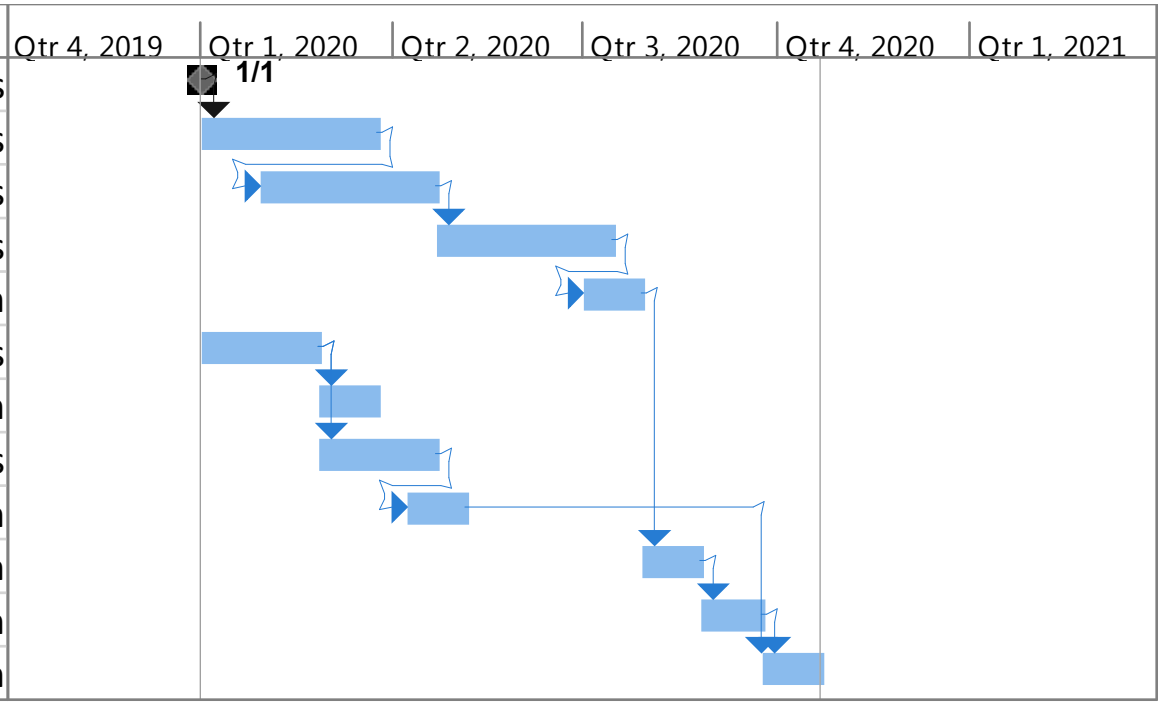
ID	Task Name	Duration
1	Intel	0 days
2	Write Spec	3 mons
3	Synthesize Threa	3 mons
4	Collect Data	3 mons
5	Provide Data	1 mon
6	Develop ATR	2 mons
7	Test Detection	1 mon
8	Test for Field	2 mons
9	ECO	1 mon
10	Deploy	1 mon



- Got it under a year!
- Is there anything else we can do?
  - Early ATR

Parallelized early ATR

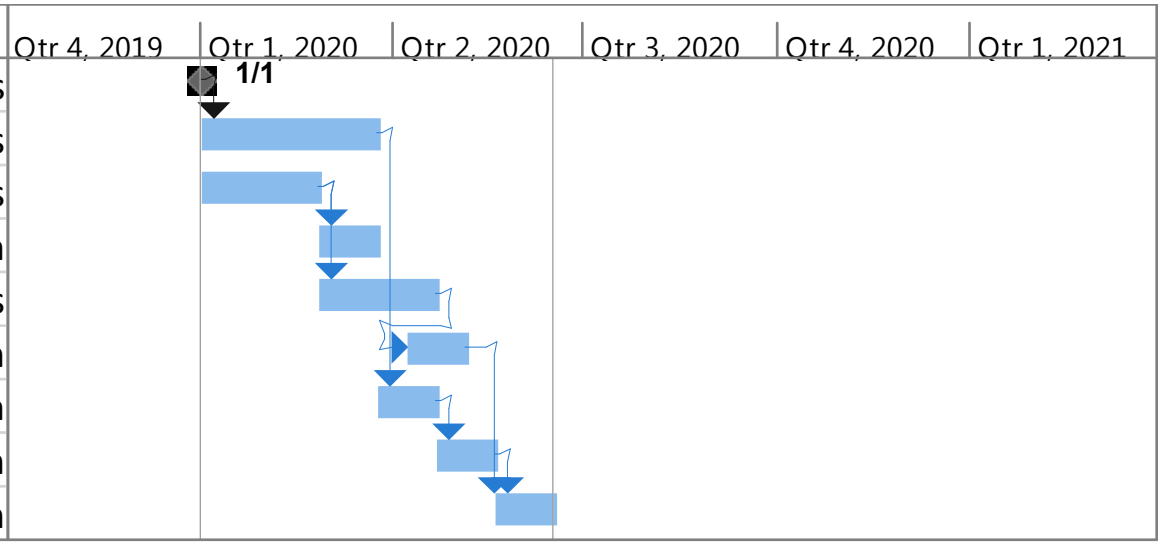
ID	Task Name	Duration
1	Intel	0 days
2	Write Spec	3 mons
3	Synthesize Threa	3 mons
4	Collect Data	3 mons
5	Provide Data	1 mon
6	Develop ATR	2 mons
7	Test Detection	1 mon
8	Test for Field	2 mons
9	ECO	1 mon
10	Final Tune	1 mon
11	Final Check	1 mon
12	Deploy	1 mon



- What if we don't need data?

Parallelized early ATR without data

ID	Task Name	Duration
1	Intel	0 days
2	Write Spec	3 mons
3	Develop ATR	2 mons
4	Test Detection	1 mon
5	Test for Field	2 mons
6	ECO	1 mon
7	Final Tune	1 mon
8	Final Check	1 mon
9	Deploy	1 mon



- What is needed to achieve this?
  - ATR that is pre-validated and can be updated without data
  - AATR

Burning Questions – The Three Gorillas

- The Market is the 800 lb. gorilla
  - How do vendors fit in?
  - How can we apply experience and expertise?
  - Talk fast, fail faster
- Integration is the invisible 800 lb. gorilla
  - How do we present adapting results in a world with CommonGUI?
  - How do we handle computation and sandboxing?
  - Early integration is key
- Validation is the invisible 8000 lb. gorilla with poisonous fangs
  - How do we pre-validate?
  - Can we ensure (relative) robustness?
  - (When) can we adapt without data?
  - Keep trying

You said “Same-Day”

- Can’t accelerate threat specification (see Larry McMichael’s talk)
- Can accelerate development (automated) and testing (automated)
- Can build and field prototypes and revise

- Risk-aversion is the invisible 8 ton gorilla with…
  - Need mechanism to field and roll-back “instantaneously”
  - How do we control that?

  - Should we fast-field an approach to fast-fielding?

Thank You