Twitter Thread by Robert M. Lee



Robert M. Lee
@RobertMLee



A quick thread on intelligence analysis in the context of cyber threat intelligence. I see a number of CTI analysts get into near analysis paralysis phases for over thinking their assessments or over obsessing about if they might be wrong. (1/x)

Consider this scenario. A CTI analyst identifies new intrusions and based on the collection available and their expertise note that the victims are all banks. Their consumer wants to know when threats specifically target banks (not just that banks are victims).

The CTI analyst has, from their collection, at this time, and based on their expertise enough to make an activity group (leveraging the Diamond Model in this example) that meet's the requirement of their consumer. So what's the problem?

The CTI analyst begins to over think it. "What if I had more collection? Would my analysis change? I really don't *know* they aren't also targeting mining companies in Australia as I don't have collection there."

The analyst knows their analysis is going to be shared. Maybe even public. "What if another team or professional intelligence firm has more collection and ends up noting that it isn't banking specific at all. Banks are victims, not targets. Will my consumer distrust me later?"

It's a scenario I see often. I see many of my #FOR578 students run into scenarios like this. "What if I say something about ICS, what will Dragos say. What if I say something about this APT, what will FireEye say. What if I say something about $X, what will CrowdStrike say."

All of our assessments are made using our expertise at a point in time with the available collection. One of the values of estimative language is explicitly accounting for the gaps. If you have significant collection gaps, bake that into the assessment: e.g. Low Confidence

Too many analysts and consumers look for facts. Intelligence is analysis. It's allowed to evolve and change as collection, time, or other considerations change. We're advising consumers to help them make better choices. Not to know the unknowable.

I would advise that analyst to make the group. Sure they can always try to coordinate with others, share, see if other groups/teams see what they see or can expose collection gaps, etc. But that's not always necessary or possible.

One of my favorite articles is the Fifteen Axioms of Intelligence Analysts by Frank Watanabe. It's been in my CTI class for years now as the last slide of the course: https://t.co/45kzw5kLz7

He doesn't start off with anything about being wrong. Or making mistakes. He starts off with "Believe in your own professional judgements." The #2 is "Be aggressive, and do not fear being wrong." It's not until #3 we hear "It is better to be mistaken than to be wrong."

Build confidence with yourself. Then build trust with your consumer. That you are going to deliver the best judgement based on the insights you have at that time. And that if it changes, you'll let them know and admit it. That's really hard to do - but it's vital.

Don't sit on your intelligence and not disseminate it, or overthink it to even finishing your work, if it can be valuable to your consumer. It's always a point in time and based on what you know at that time. You'll never have enough to feel comfortable

The balance is in not blasting your consumer with thinly supported guesses though. Go through your processes. Use your team. "Aggressively pursue collection of information you need." But then make the call. If it was easy it wouldn't be intelligence.