Breaking down barriers:

Using an intelligence mindset no matter who you are

Katie Nickels

VB2021 localhost

red canary

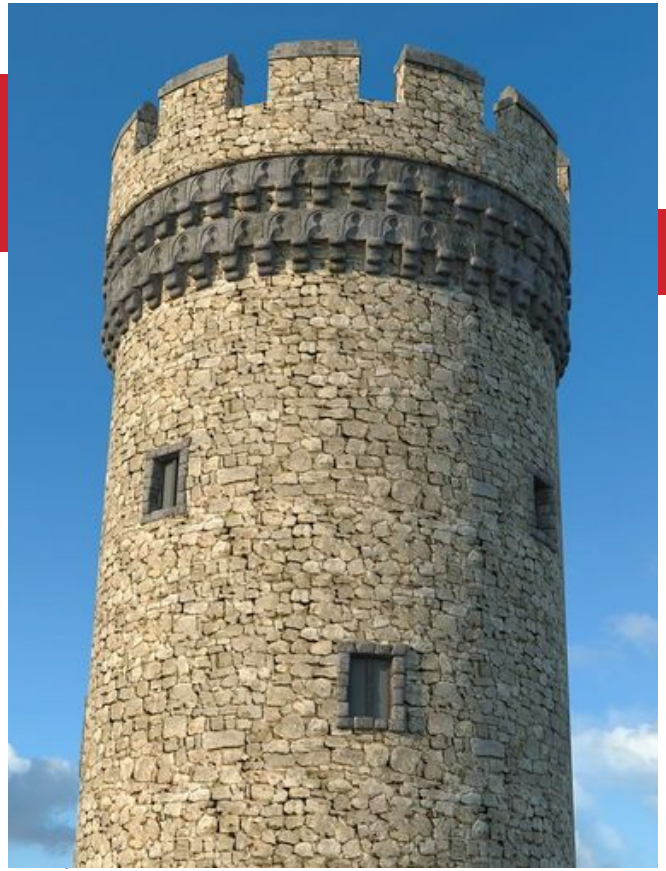
About me

Katie Nickels
DIRECTOR OF INTELLIGENCE
RED CANARY

@LiketheCoins

- SANS Certified Instructor for FOR578: Cyber Threat Intelligence
- Non-Resident Senior Fellow for the Atlantic Council's Cyber Statecraft Initiative
- Bringing context about threats to inform better decisions
- Chocoholic and CrossFitter

red canary



Intelligence seems like it sits in an ivory tower

red canary

But it can help
all of us improve
our thinking

red canary

Things intel analysts do

...that you can do too!

- Make assessments
- Avoid brain tricks
- Consider other possibilities
- Respond to requirements
- Attribute threats

red canary

Make assessments

red canary

Making assessments

1. Properly describe the quality and credibility of underlying sources, data, and methodologies
2. Properly express and explain uncertainties associated with major analytic judgments
3. Properly distinguish between underlying intelligence information and analysts assumptions and judgements
4. Incorporate analysis of alternatives
5. Demonstrate customer relevance and address implications
6. Use clear and logical argumentation
7. Explain change to or consistency of analytic judgements
8. Make accurate judgments and assessments
9. Incorporate effective visual information where appropriate

https://www.dni.gov/index.php/how-we-work/objectivity

Assessments, simplified

- **I think X because of Y**
- This isn't speculation — there's a reason you think that
- Example:
  - "I think this is TrickBot because of a tweet from the Malware Hunter Team that says the C2 IP is TrickBot."

Avoid brain tricks

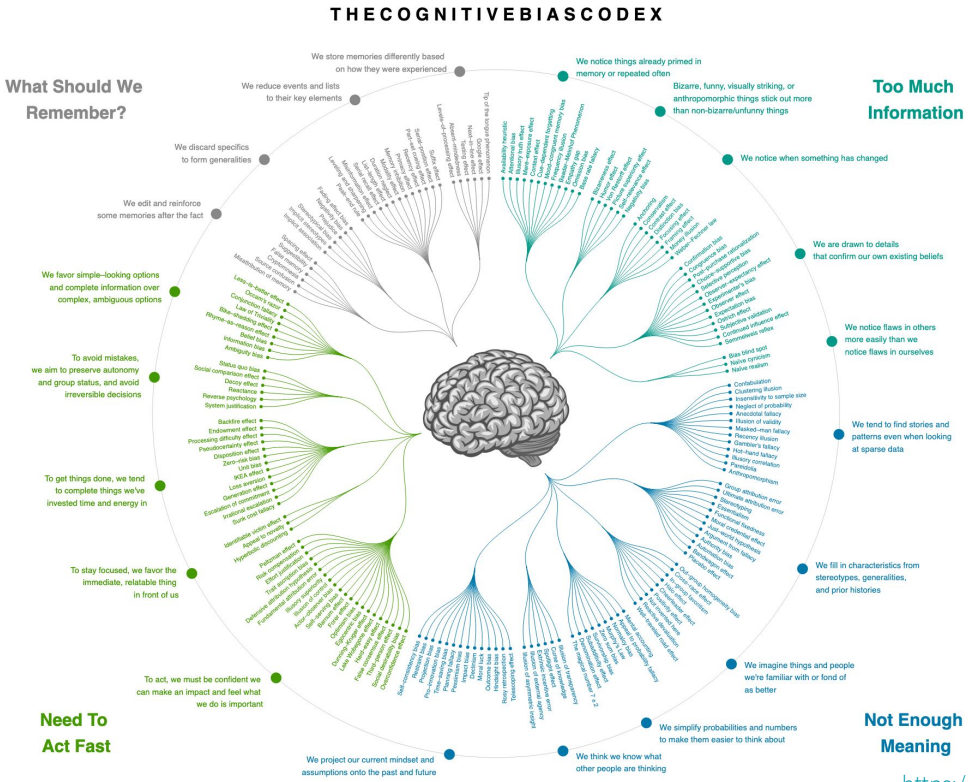
red canary

What do these triangles say?

https://www.cia.gov/static/9a5f1162fd0932c29bfed1c030edf4ae/Pyschology-of-Intelligence-Analysis.pdf

red canary

So many cognitive biases



- Confirmation bias
- Anchoring
- Availability bias

https://commons.wikimedia.org/wiki/File:Cognitive_bias_codex_en.svg

red canary

Cognitive biases, simplified

- Slow your roll
- Surround yourself with people who challenge your thinking
- Example:
  - You: “This is probably TrickBot because the first tweet I read said it was.”
  - Your teammate: “Are you sure? Do you have other evidence?”

red canary

Consider other possibilities

red canary

ACH

Analysis of
Competing
Hypotheses

Question: Will Iraq Retaliate for US Bombing of Its Intelligence Headquarters?

Hypotheses:
H1 - Iraq will not retaliate.
H2 - It will sponsor some minor terrorist actions.
H3 - Iraq is planning a major terrorist attack, perhaps against one or more CIA installations.

	H1	H2	H3
E1. Saddam public statement of intent not to retaliate.	+	+	+
E2. Absence of terrorist offensive during the 1991 Gulf War.	+	+	−
E3. Assumption that Iraq would not want to provoke another US attack.	+	+	−
E4. Increase in frequency/length of monitored Iraqi agent radio broadcasts.	−	+	+
E5. Iraqi embassies instructed to take increased security precautions.	−	+	+
E6. Assumption that failure to retaliate would be unacceptable loss of face for Saddam.	−−	+	+

https://www.cia.gov/static/9a5f1162fd0932c29bfed1c030edf4ae/Pyschology-of-Intelligence-Analysis.pdf

red canary

Hypotheses, simplified

- What are some other explanations?
- What evidence is making me think a certain answer is right?
- What if that evidence is wrong?
- Example:
  - “I think this is TrickBot based on this C2 IP, but it might be Qbot. I’m going to look beyond that single tweet.”

red canary

Respond to requirements

red canary

Intelligence Requirements

1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence.
2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces.

https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

red canary

Requirements, simplified

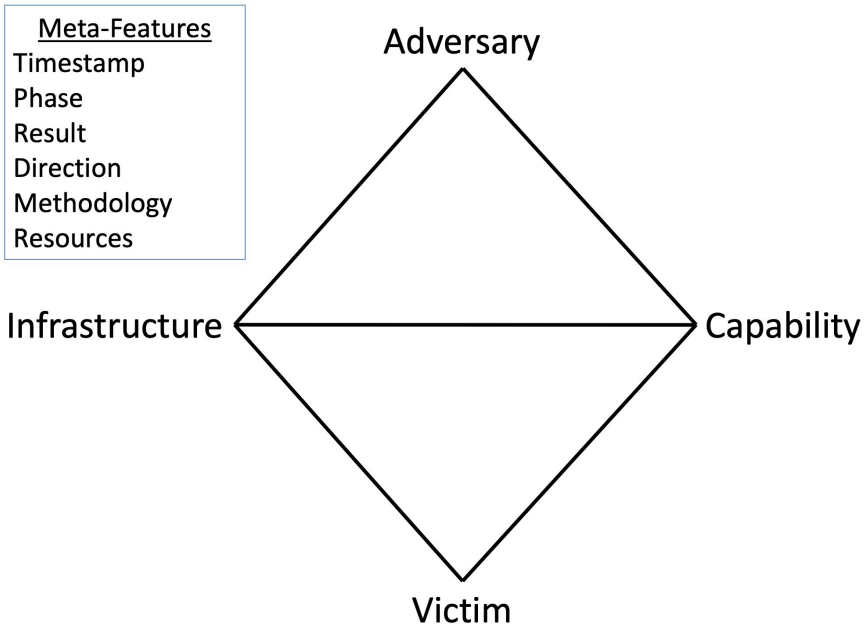
- Why are you doing what you're doing?
- Who will use it?
- How could you make it more useful to them?
- Example:
    - "I'm writing this malware report on TrickBot for our detection engineers. They don't care about the API calls, so I'm going to focus on behaviors."

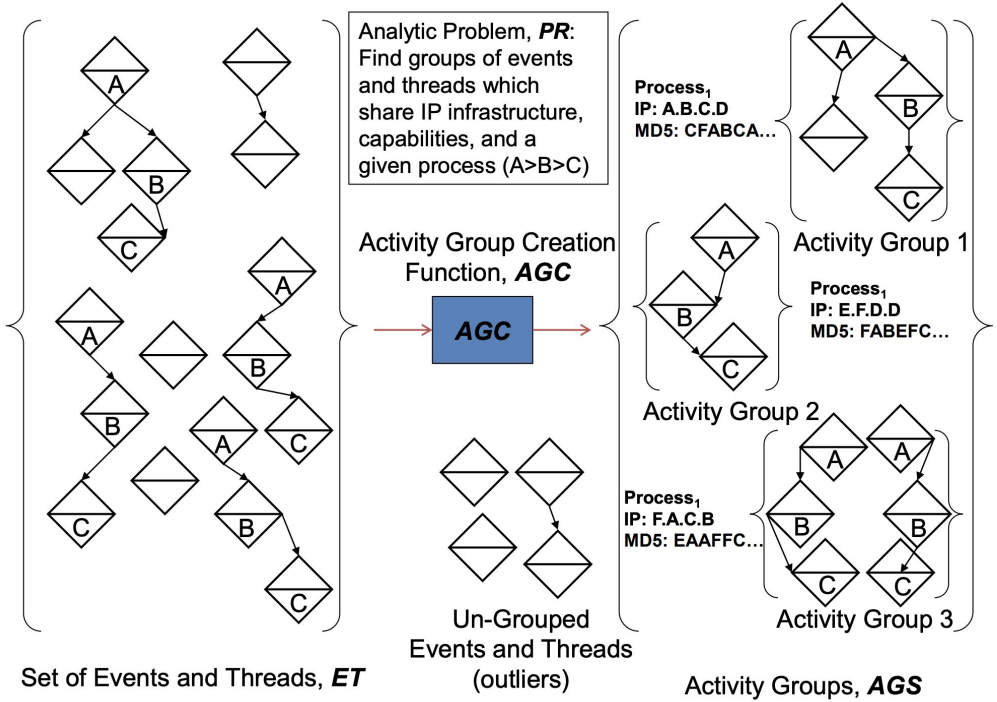
red canary

Attribute threats

red canary

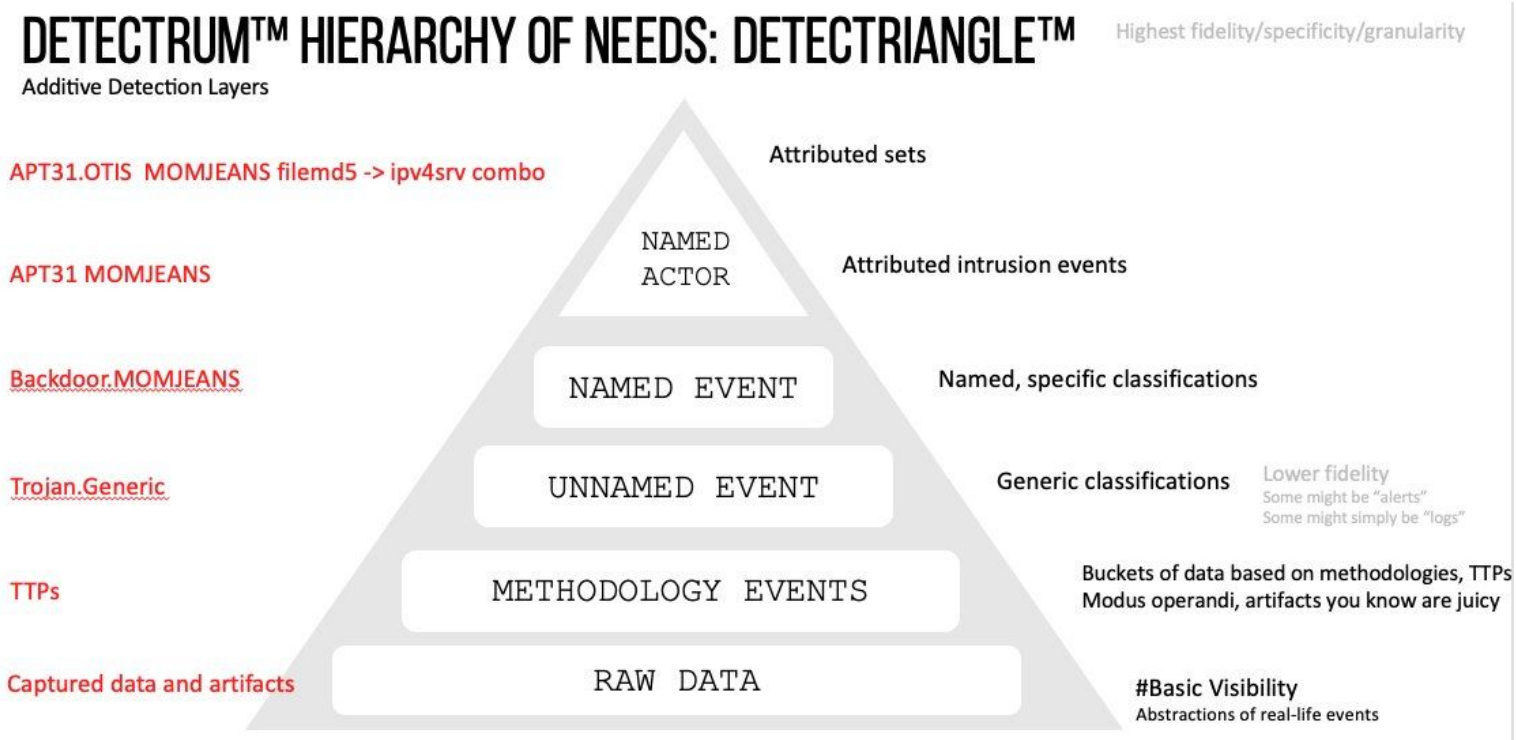
Attribution can be hard





https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Different levels of attribution



https://twitter.com/stvemillertime/status/1405226952739352580/photo/1

Attribution, simplified

- Why do you think it's a certain group or malware family?
- How many points of overlap do you have?
- How unique are the overlaps?
- Example:
  - "I see that this C2 IP has been used by TrickBot, but based on further research, it has also been used by Qbot. I'm going to look for other overlaps before deciding which family this is."

red canary

Wrapping up

red canary

Takeaways

- Explain why you think what you think
- Slow down to avoid brain tricks
- Consider other explanations
- Think about why you're doing what you're doing
- Identify overlaps in threats

red canary

Thank you!

Katie Nickels
DIRECTOR OF INTELLIGENCE
RED CANARY

@LikethеCoins

red canary