

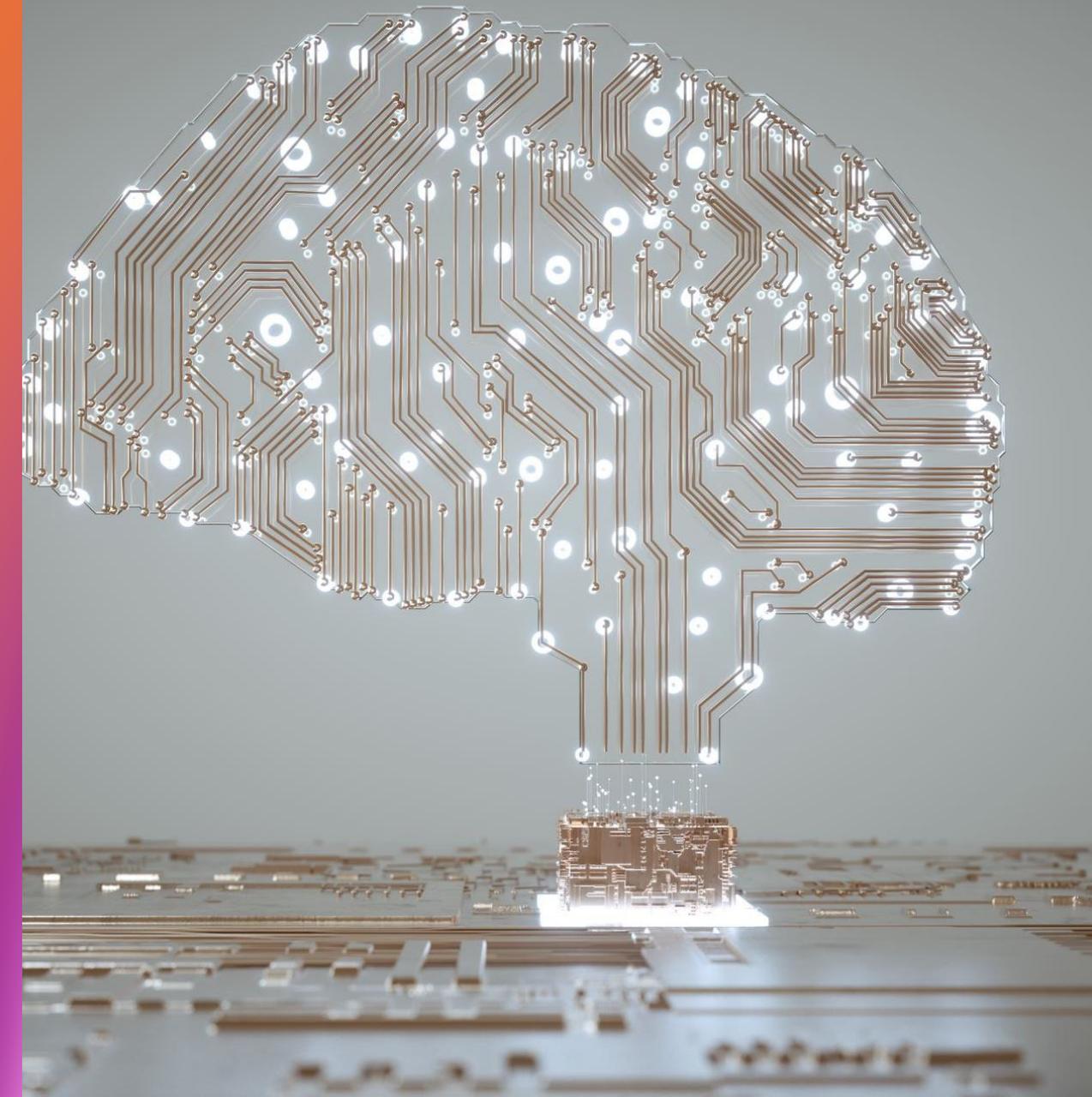


What the heck are Hermeneutics?

...and how you can use this to level up your
CTI game

Intro – Training session

- What exactly did you get yourself into for the next 40 mins.
- We are going to learn about Cyber threat intelligence
- How to use skills you may already have to create finished intelligence
- Where and how to practice your skills
- Why liberal arts are the missing element of CTI and Cyber
- And of course.. What the heck is Hermeneutics



Reflection – Why Cyber Threat Intelligence

For me.. it's the Aha moments which is the heart of information sharing.

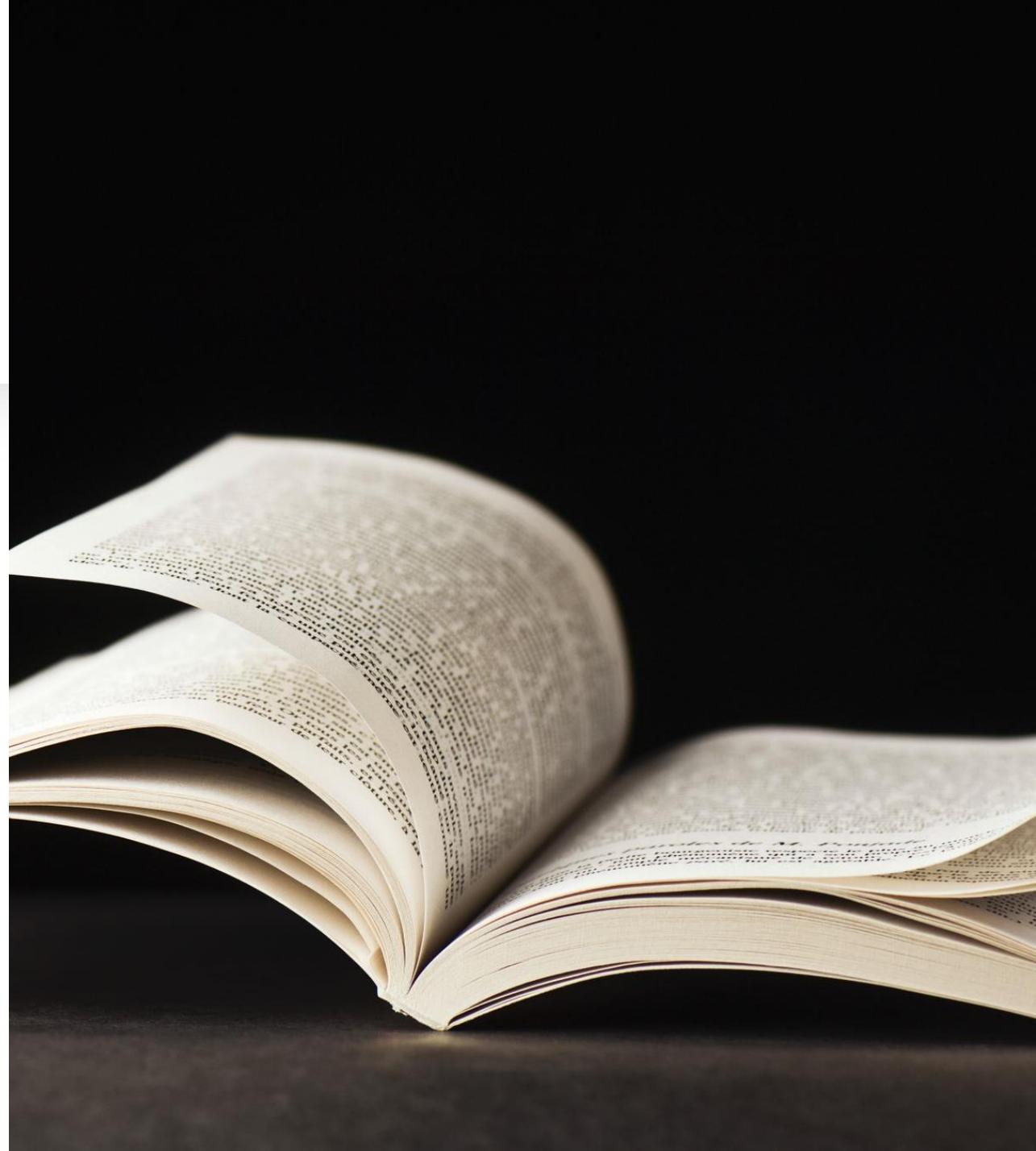
Hermeneutics

From Wikipedia

Hermeneutics: is the theory and methodology of interpretation especially the interpretation of biblical texts, wisdom literature, and philosophical texts. As necessary, hermeneutics may include the art of understanding and communication.

Modern hermeneutics includes both verbal and non-verbal communication as well as semiotics, presuppositions, and pre-understandings. Hermeneutics has been broadly applied in the humanities, especially in law, history and theology.

Hermeneutics – As a framework for creating finished intelligence



Hermeneutics fundamentals

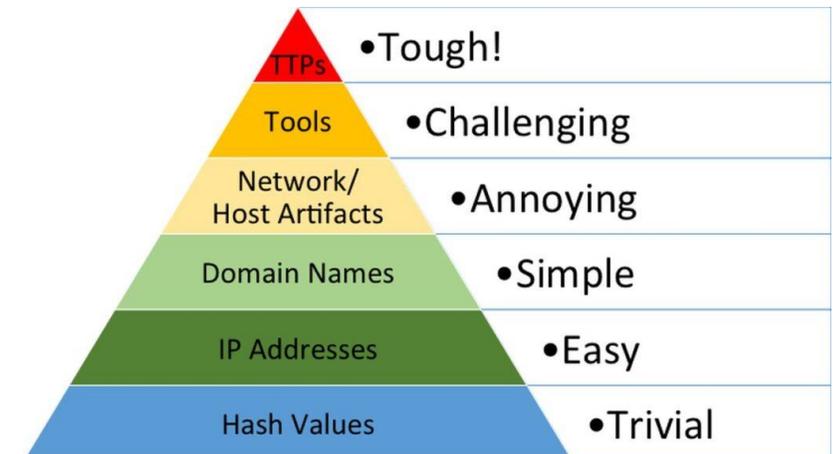
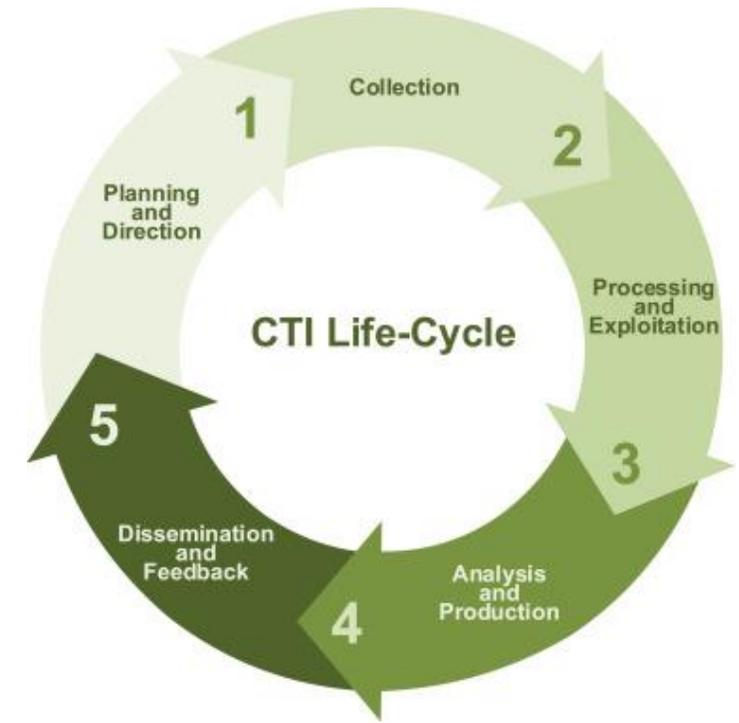
Hermeneutics circle

Presuppositions

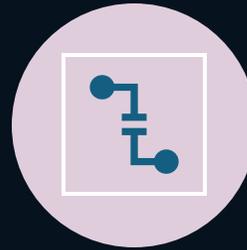
Signs and symbols –
(Emoji's and Memes)

What CTI training looks like today

Lifecycle + Pyramid = Profit



Congrats you're
all now threat
analysts!!



NOW WHAT?

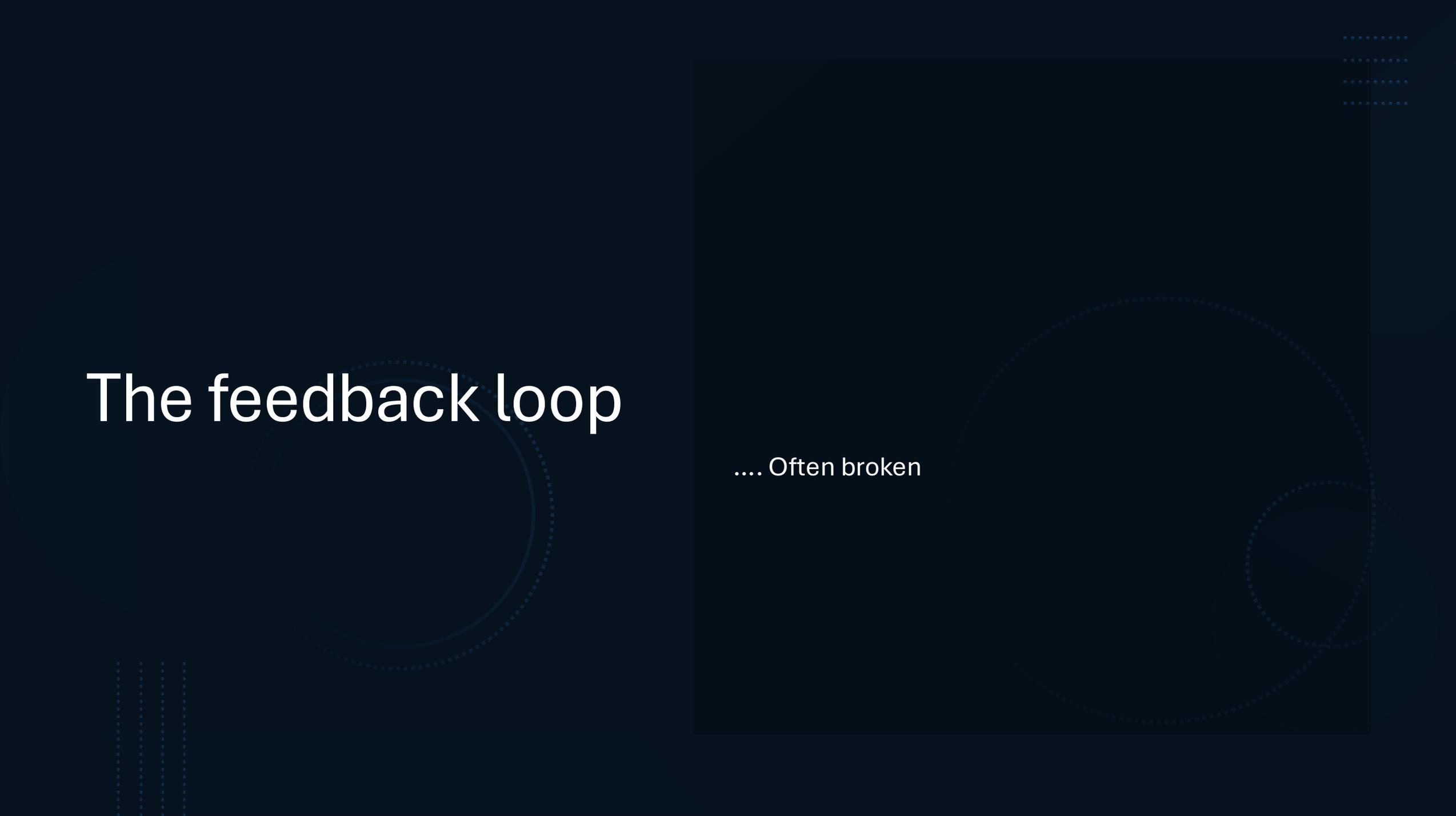


HOW DO YOU CREATE
FINISHED
INTELLIGENCE?



WHERE DO YOU
START?

The feedback loop

The background is a dark blue gradient. It features several decorative elements: a large dotted circle on the left side, a smaller dotted circle on the right side, and a vertical dotted line on the far right edge. There are also some faint dotted lines in the bottom left corner.

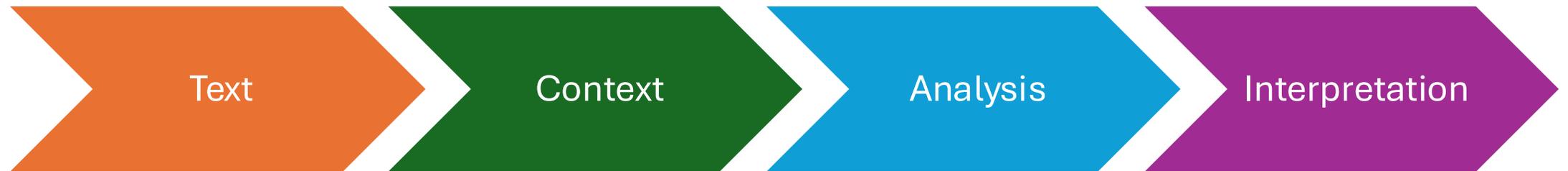
.... Often broken

Still a circle?

Source: A Roadmap for SMEs to Adopt an AI Based Cyber Threat Intelligence.



Visualizing the analysis process



The problem with AI

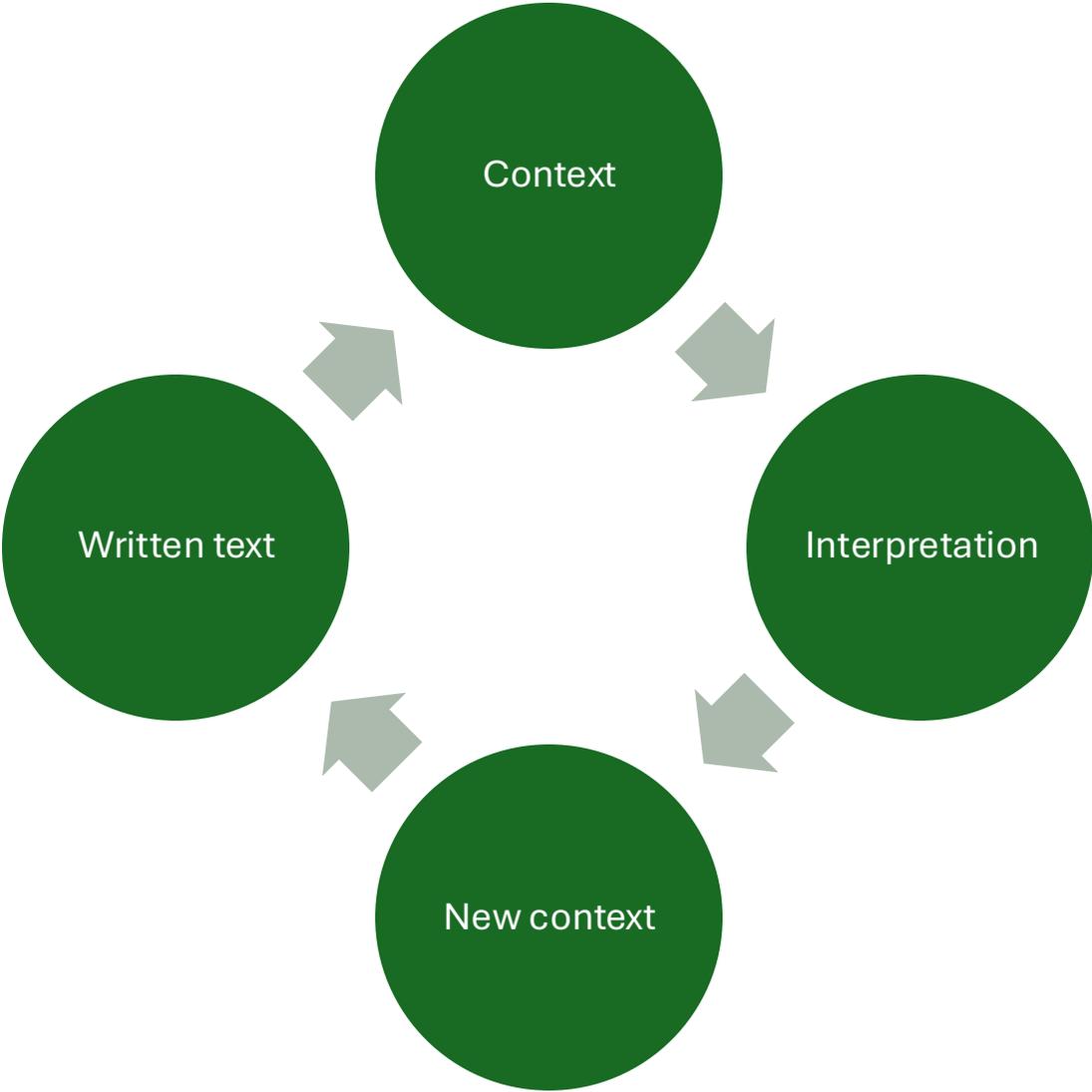
If AI developers don't understand the how and why of what makes good intelligence. How can we expect them to train the models to produce the end product we are looking for?

Not a linear process

Text must be revisited when:

- Challenging bias
- When provided with new information
- Considering differing points of view
- If the process were linear – How would we be able to change our mind when presented with new information.

The hermeneutic circle



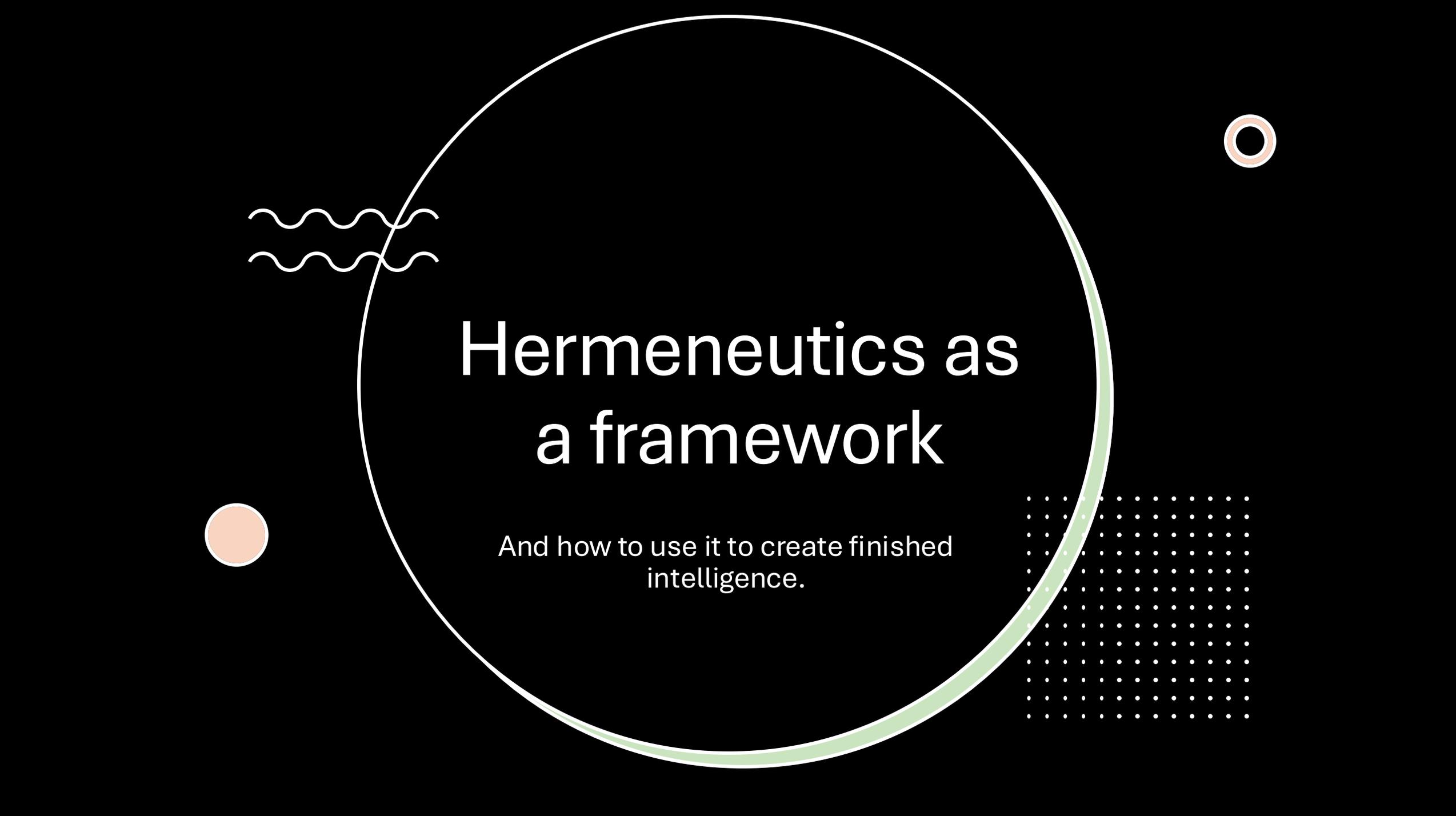
Have a Human In the loop

AI's answer of how things SHOULD work!

If done well – AI in CTI

- Amazon Fresh – Just walk out stores.





Hermeneutics as a framework

And how to use it to create finished
intelligence.

Why the why?



Understanding priorities.



Answering the question – Why is this important. And how will this information help you.

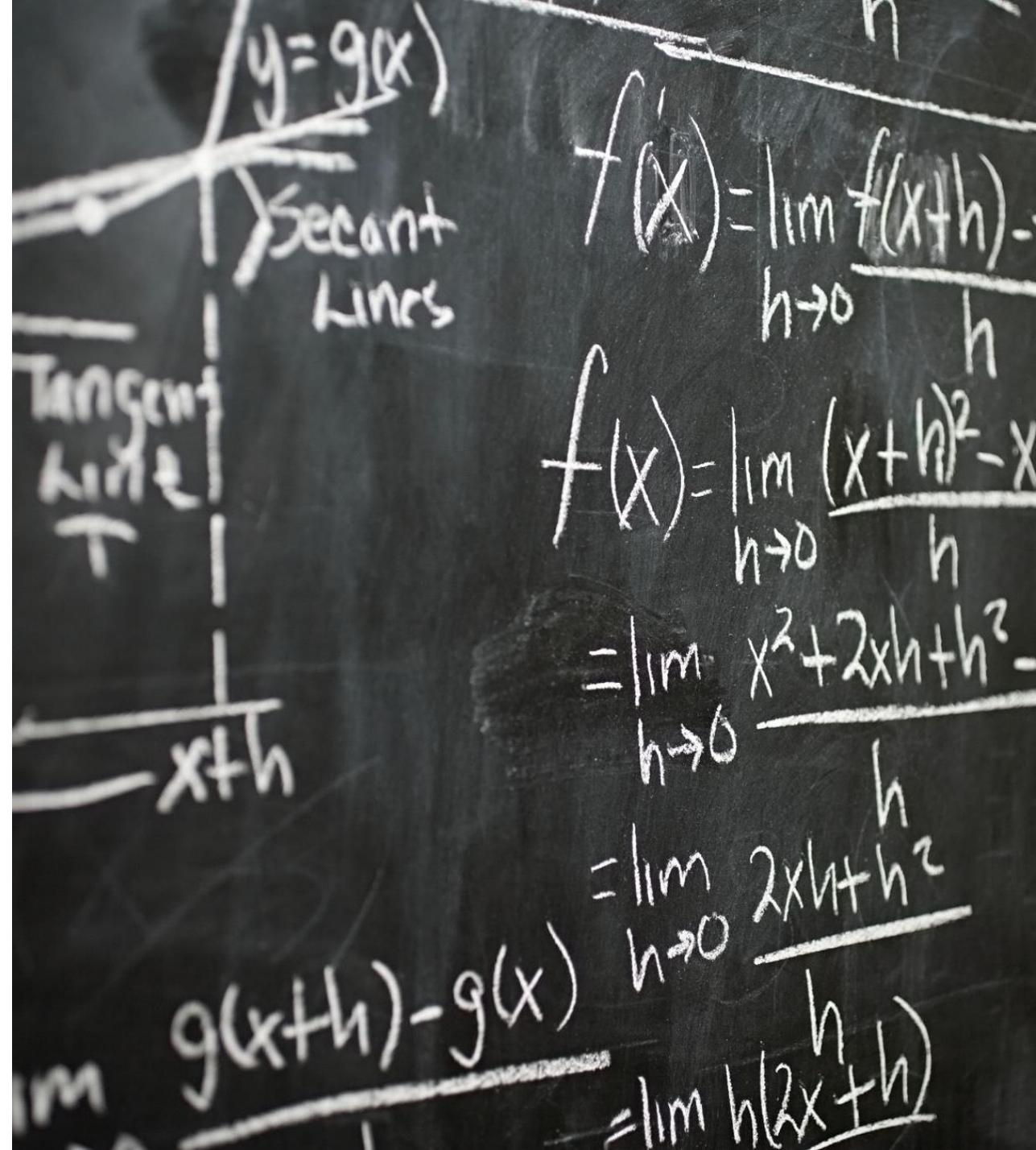
Where to start?

- Understand the objectives of the entity you are providing the intelligence to.
- Find the fallacies – it may be important to call them out
- Limit your information to only what is needed. Respect time and resources of the people, organizations, you are sharing the information with.



Presuppositions

Be aware of the fallacies of built-in presuppositions

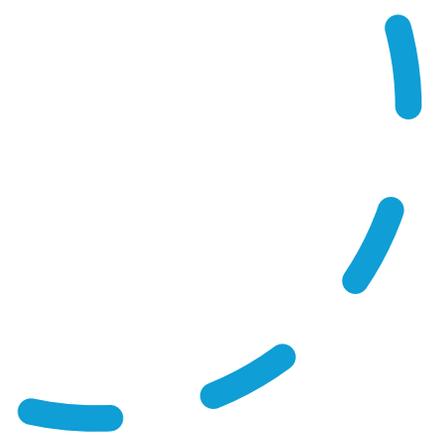


... ..
+++++

- If you refuse to cooperate with us, it will lead to the following consequences for your company:
1. All data downloaded from your network will be published for free or even sold
 2. Your system will be re-attacked continuously, now that we know all your weak spots
 3. We will also attack your partners and suppliers using info obtained from your network
 4. It can lead to legal actions against you for data breaches

.....

IF THEN



The Delivery Matters!



GIVING A BRIEFING



WRITING A REPORT



WRITING A BULLETIN



INFORMATION SHARING
CALLS (OFTEN CALLED
“STORY TIME”)

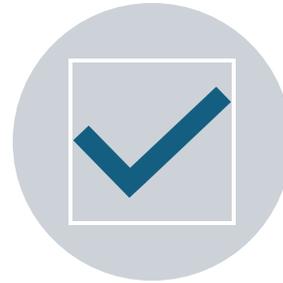
Briefings

- Keep them short and concise
- Not the time to share your credentials or all your research.
- Respect TIME!
- 3-part briefings work well

3 Part Briefings + Call to action



Each part limited to only the information necessary



Builds upon the last section



Delivered as a part of the whole



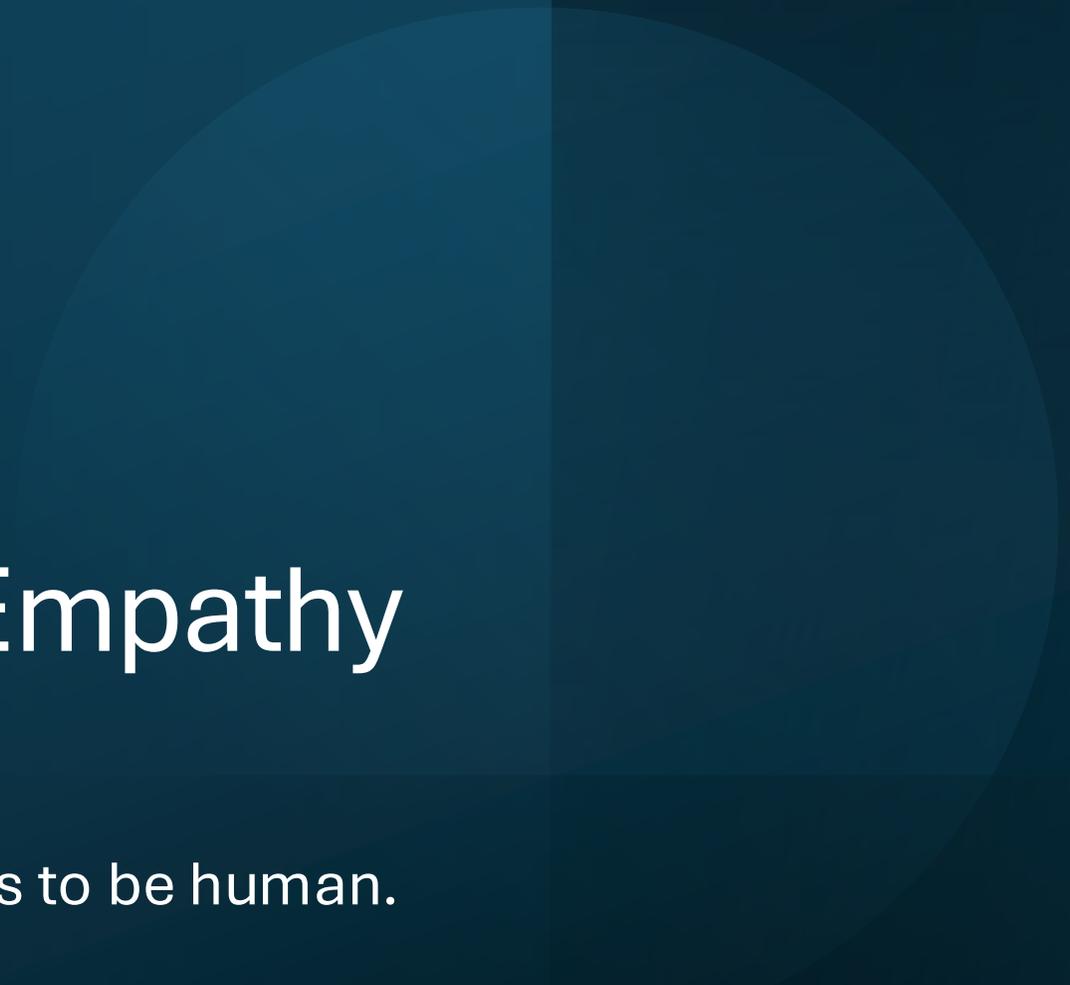
Include a final call to action

Briefing

you will have access to a detailed copy of your network data to gain access to your network
+-----+

If you refuse to cooperate with us, it will lead to the following consequences for your company:

1. All data downloaded from your network will be published for free or even sold
2. Your system will be re-attacked continuously, now that we know all your weak spots
3. We will also attack your partners and suppliers using info obtained from your network
4. It can lead to legal actions against you for data breaches



Empathy

Experience what it is to be human.

Where to practice your skills

- Social media
- Movies
- Music
- Poetry
- Art
- Philosophy
- Psychology

Thank you!

[linkedin.com/in/cherieburgett](https://www.linkedin.com/in/cherieburgett)

cburgett@mmisac.org