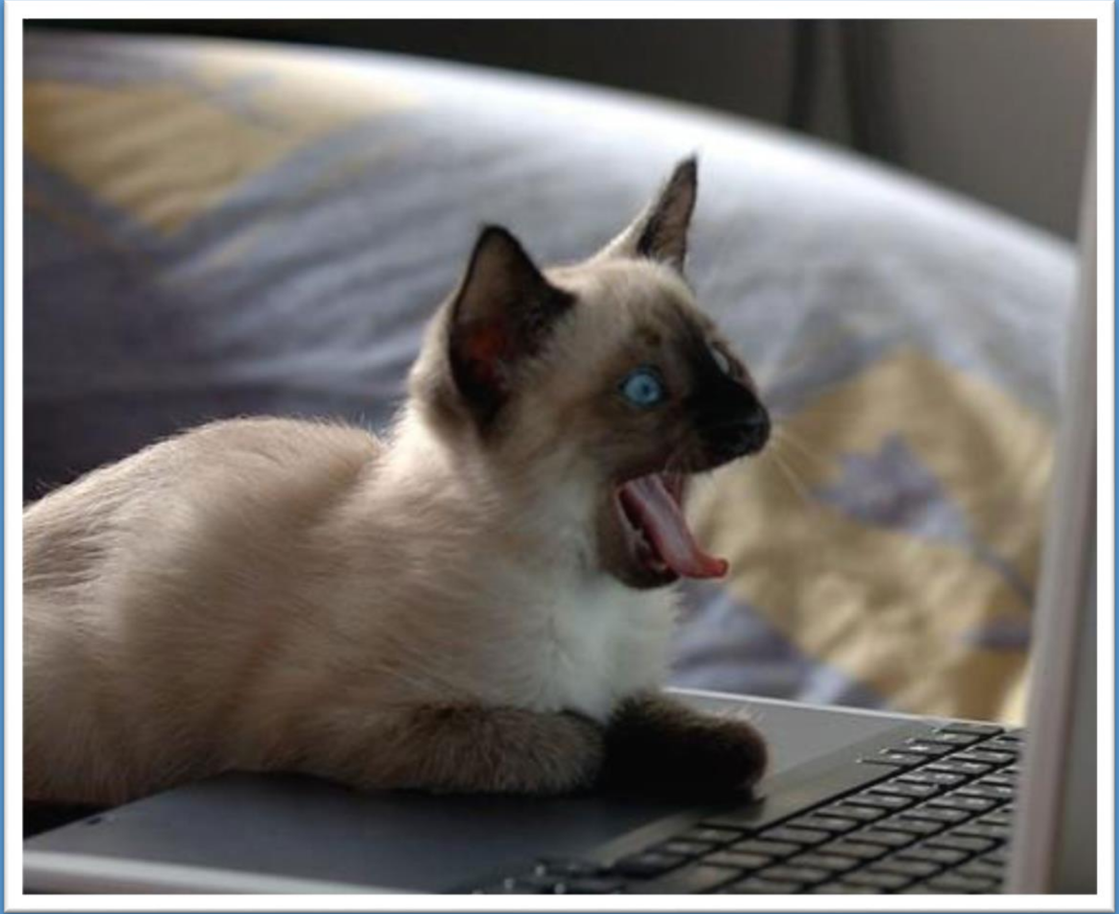
I CAN HAZ REQUIREMENTS?



Requirements and CTI Program Success

About Me

McAfee
UNITEDHEALTH GROUP®
USS PELELIU LHA 5
PAX PER POTENS
UNITED STATES CYBER COMMAND
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Search your feelings…

…you know it to be true!

Why do we need requirements?

Answer critical questions intelligence customers care about

Not what you care about

Intel requirements help you:

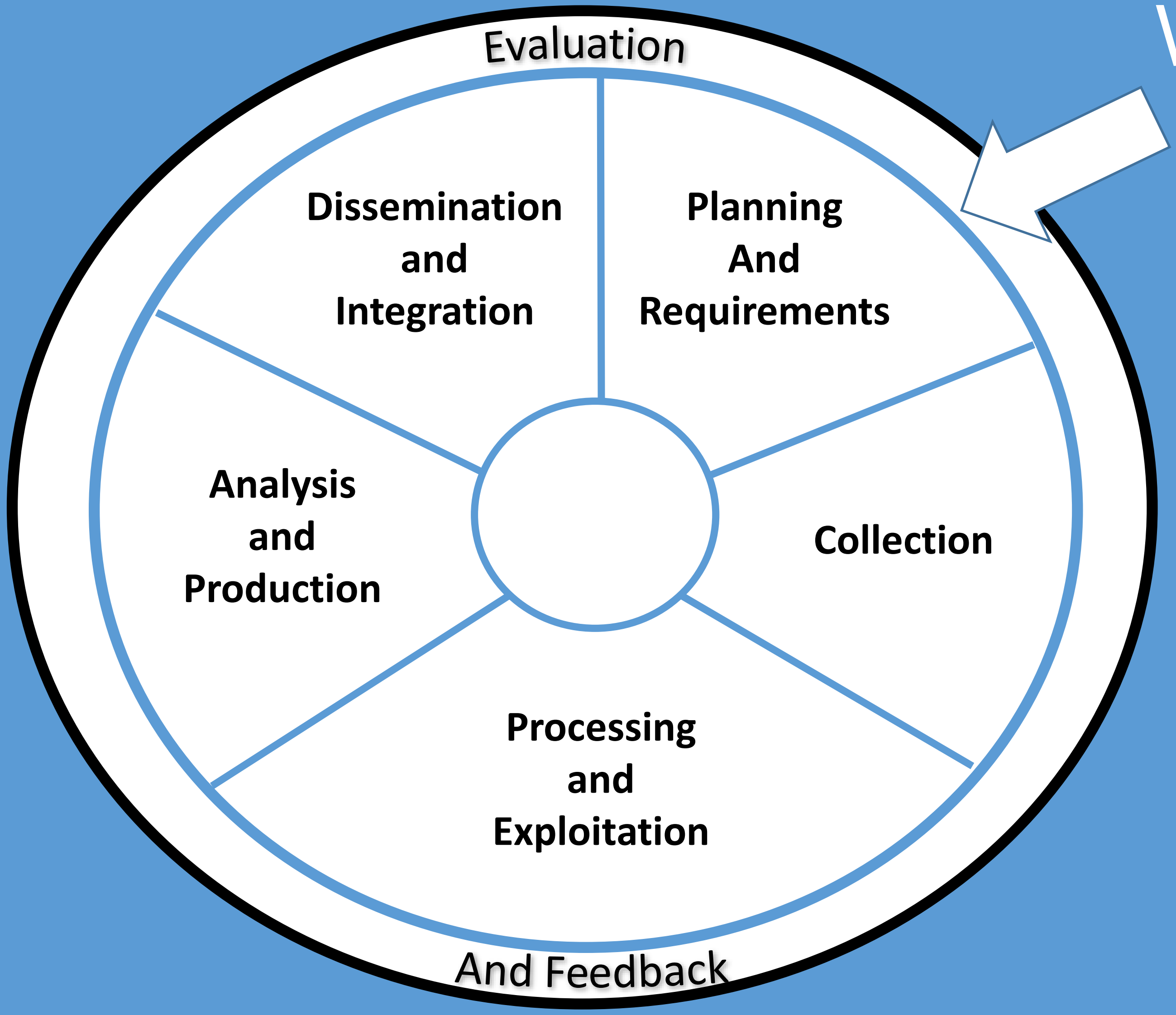
Scope deliverables

Prioritize collection

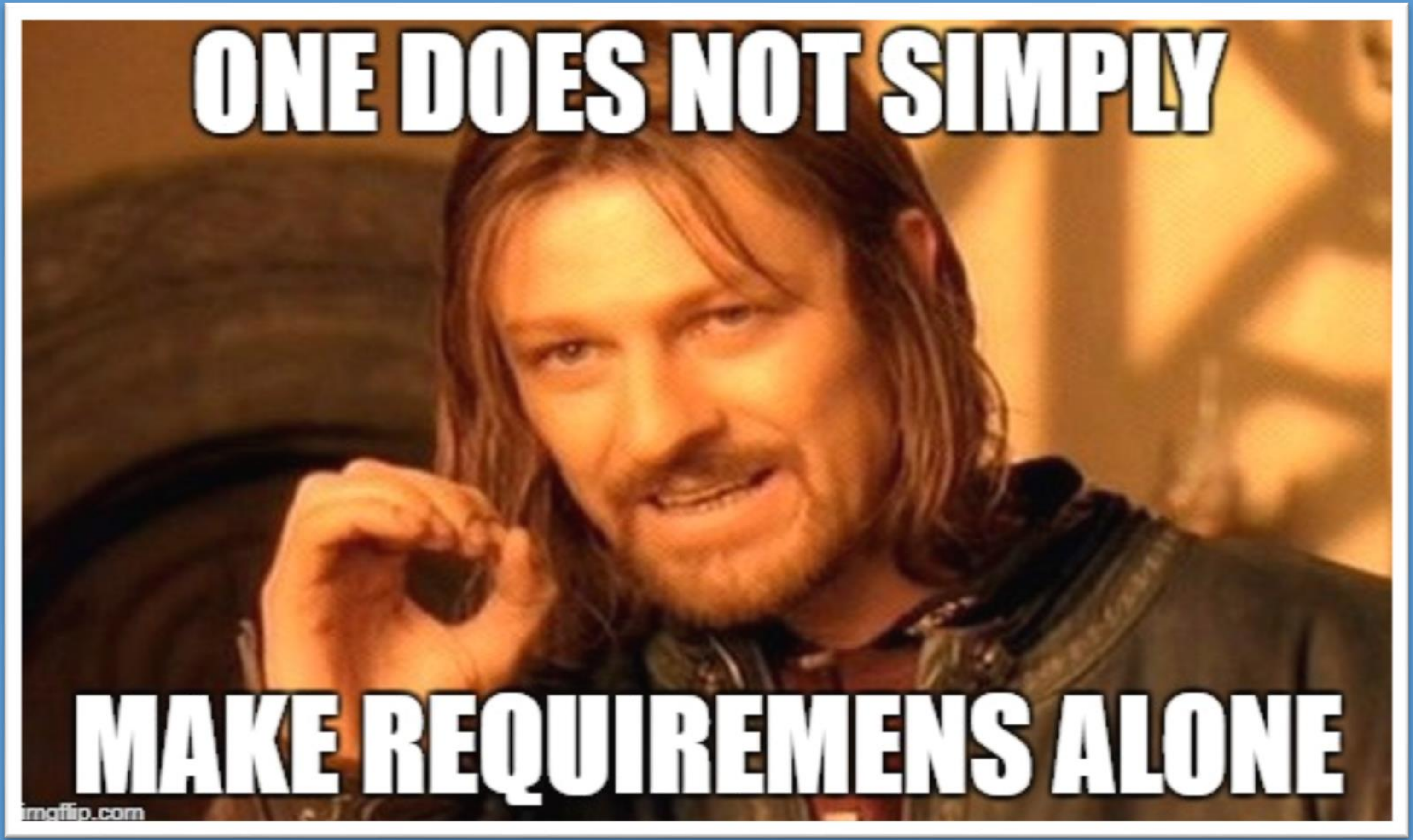
Identify needed data sources

Get ahead of the adversary

Without this

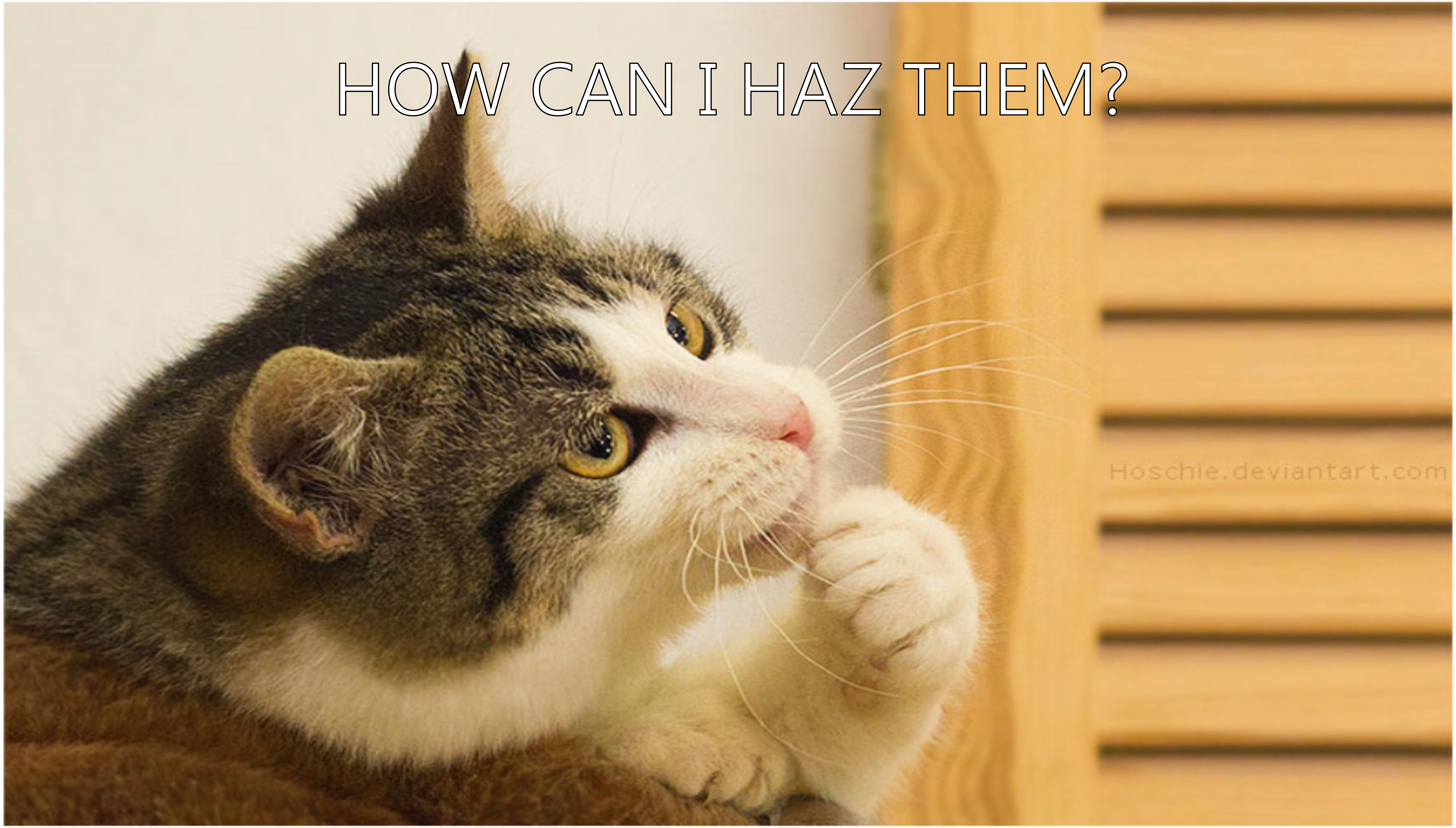

Evaluation
Dissemination and Integration
Planning And Requirements
Analysis and Production
Collection
Processing and Exploitation
And Feedback

You can’t do the rest



Let's make them together!

HOW CAN I HAZ THEM?



Identify all the stakeholders and customers who need intel support

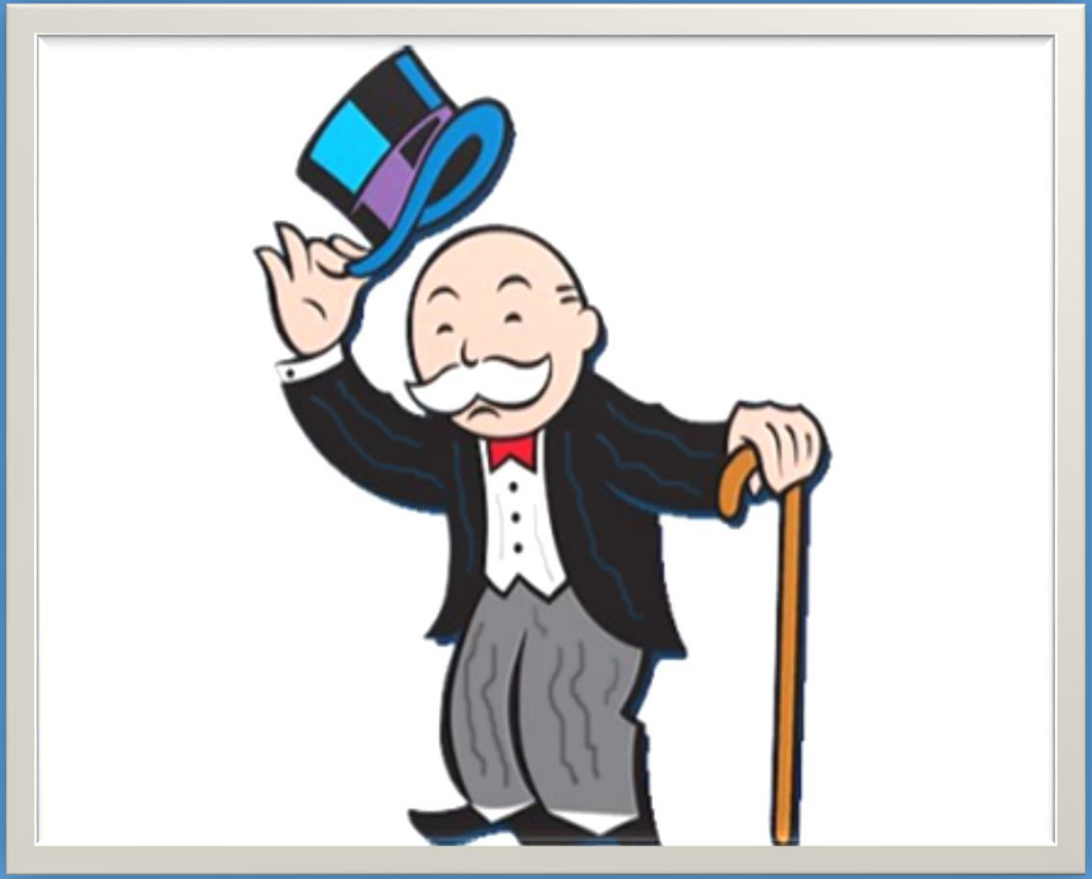
Red Team

Security Operations Center

Incident Response Team

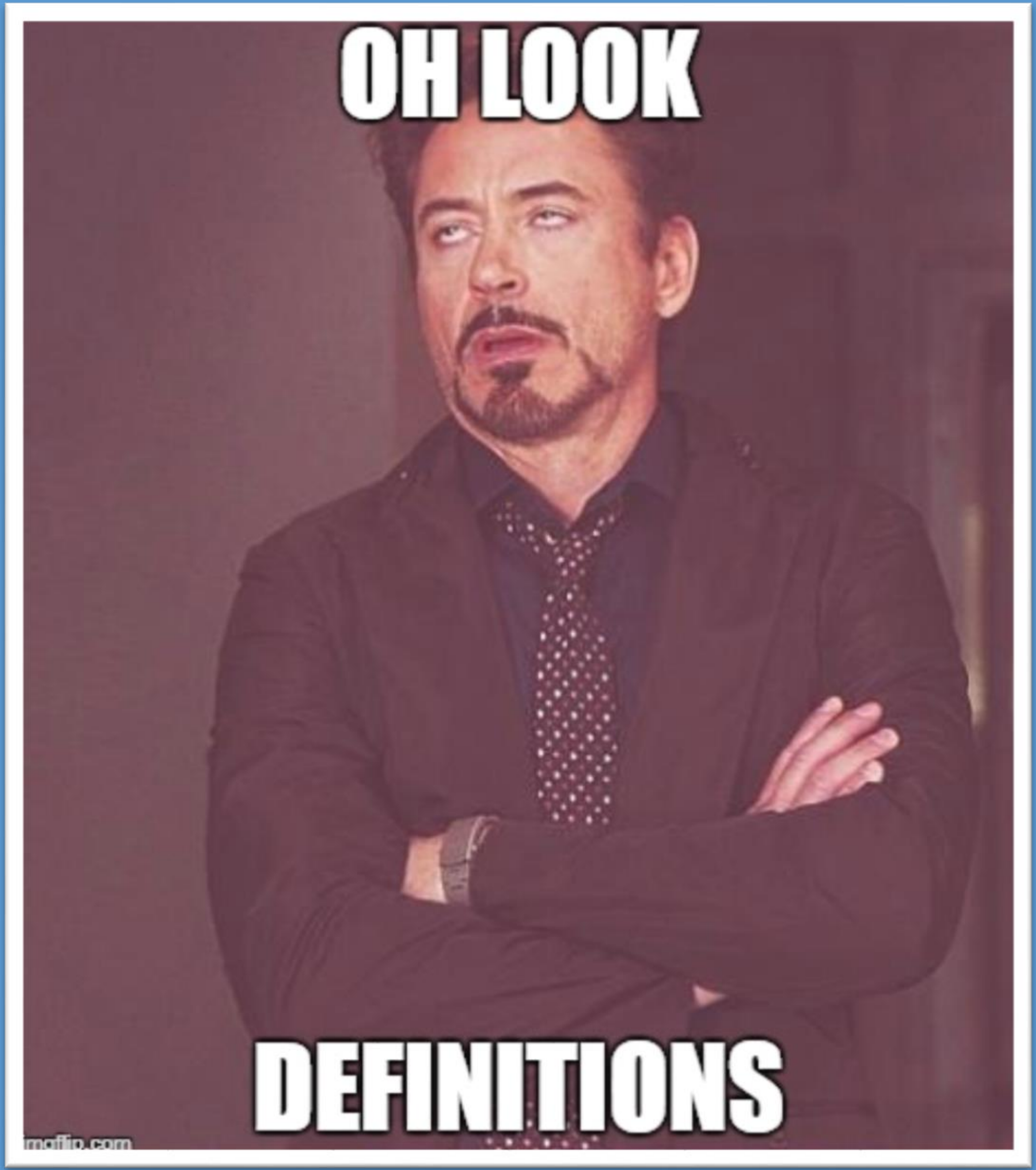
Brand Reputation

C-Suite (Hi CISO!)
Board of Directors
Policy folks



What is an intelligence ***requirement***?

“Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence.” DOD Joint Pub 2-0



What makes a *good* intelligence requirement?

Four things!

Timeliness

Aids ONE decision

Asks ONE question

Focuses on ONE activity/event/thing

Now for a

A decision can be inaction!

Where do I start?

But seriously...

How?

Who?

Why?

What?

When? Where?

BUT WAIT
THERE'S MORE!
ARM & HAMMER
Pure
Baking Soda
imgflip.com

Use your attack surface.

Model the threat.

If you haven’t done it, do it.

VICTIMS OF A FEATHER
GET INFECTED TOGETHER
imgflip.com

Something something supply chain something something.

Where in the world is Carmen…I mean you?

What stuff do you have that they want?

TLDR? Requirements are enduring questions consumers of intelligence need answers to

What do you do when someone reacts to something in the news?

The RFI Process!

Helps CTI shops manage ad-hoc intelligence needs not met by standing requirements

Without one, your team can get flooded with noise

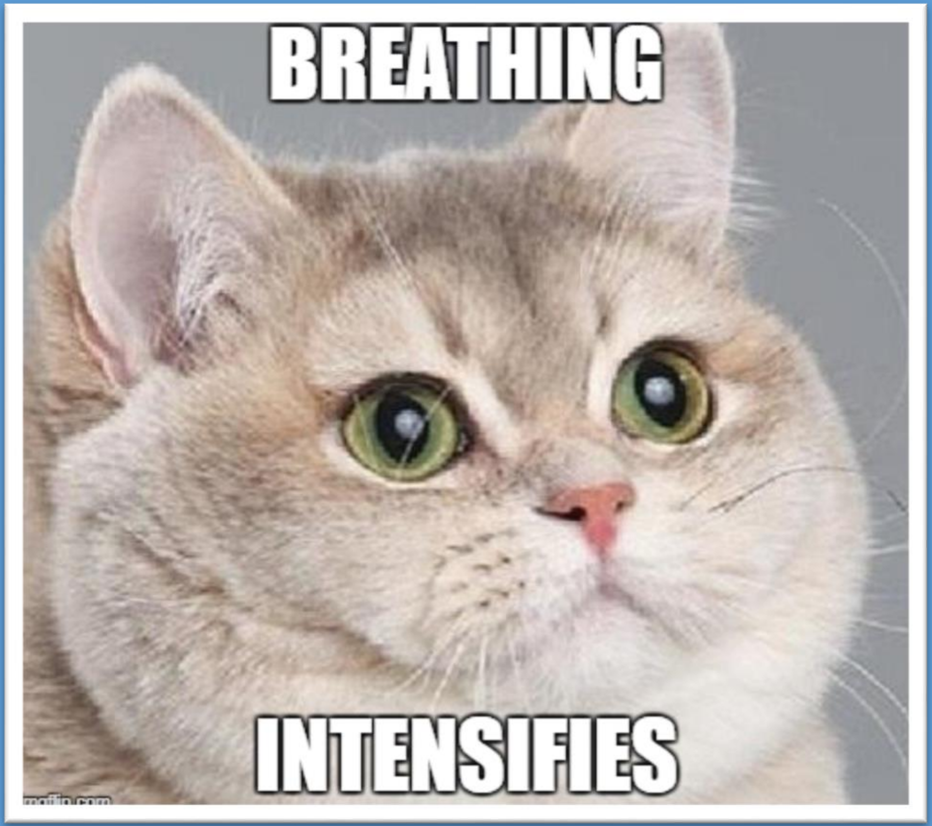
Work with customer on scoping expected deliverable

What do they need?
When?
Format?
What does it help support?

How can I track RFIs?

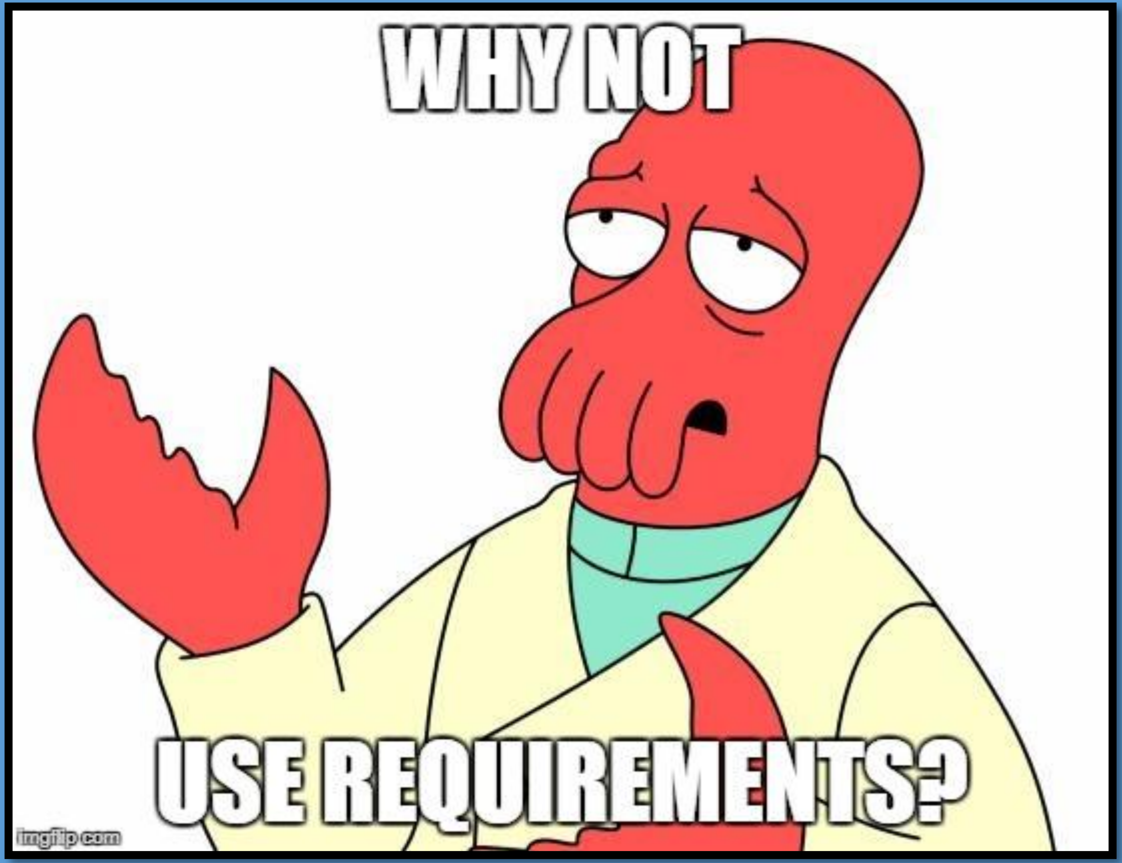
Excel (sorry)
Sharepoint Workflow (less sorry?)
Email

So I have requirements…
…now what?



Metrics!
Please don’t be like…

Metrics are often the hardest thing for CTI shops to create



You can:

Show number of products created aligned to numbered requirements
(Throw in RFI’s answered too)

You can:

Show customers where production is strongest, weakest

You can:

Identify collection/capability gaps
(Not just intel specific!)

To say what I said:

Requirements help align internal, external data sources and capabilities to specific needs

Shows where current capabilities are lacking, drives collection capability acquisition

Sets expectation of what your team is producing, when they're producing, and for whom

Takeaways:

If you're not doing this now, start the conversation

(Try to) make it a team sport

Do what we preach

You can find me on Twitter: @ComradeCookie Medium: ComradeCookie