Slow cooking & Cyber Threat Intelligence:

Cooking a High Performing Team

Gert-Jan Bruggink

SANS CTI Summit

30 January 2024

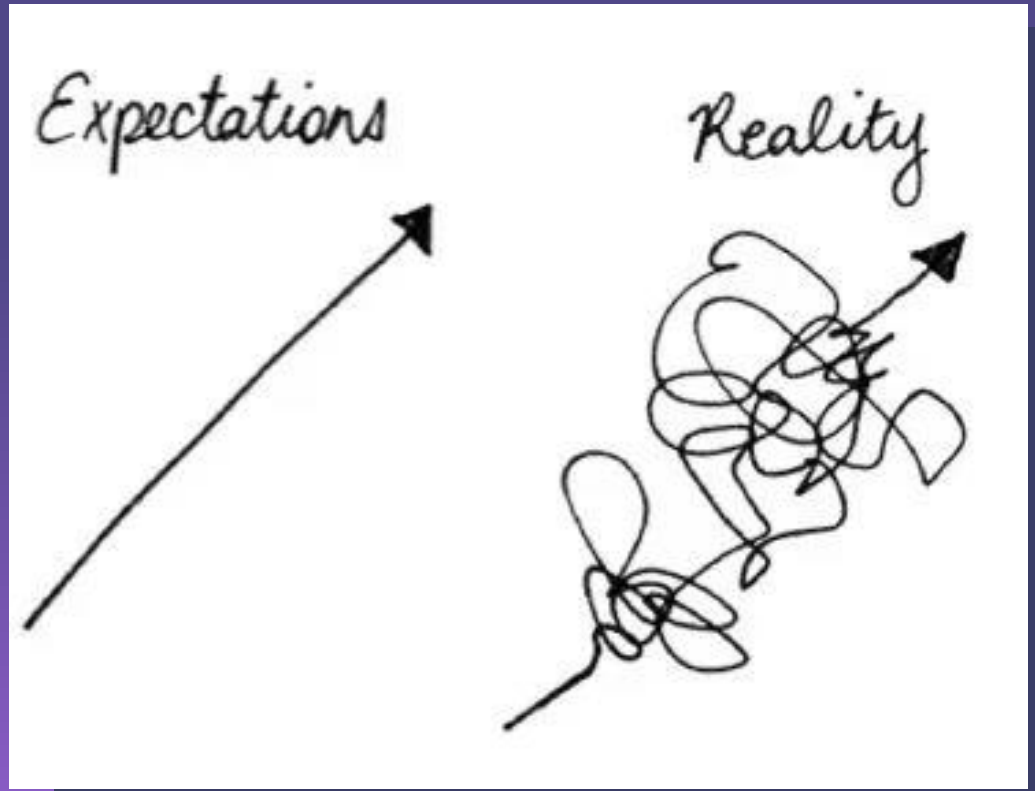
What is “Ragu’ alla Bolognese”?

What does Bolognese have in common with slow cooking, cyber threat intelligence, and building teams?

Key takeaways

- ✓ The ideal recipe for your CTI team:
  there is not one recipe
- ✓ Tune different ingredients over time:
  key to longer-term success
- ✓ Maintaining a continuous improvement mindset is crucial:
  not saying its easy

Performing at life



Source: https://believeinyourshelf.files.wordpress.com/2013/08/teen-blog1.jpg

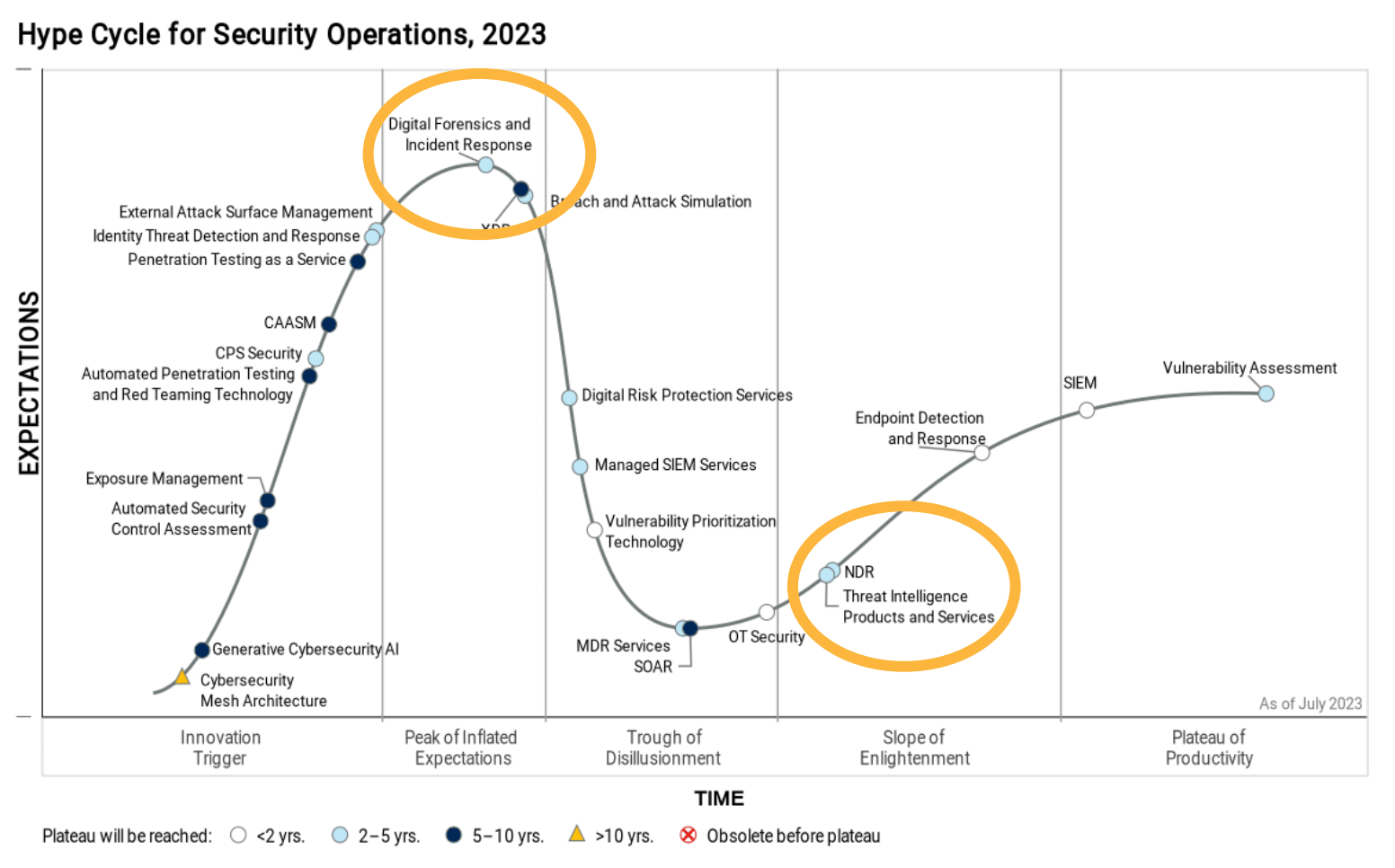
Performing vs high performing/performance

Source: https://media.licdn.com/dms/image/D4E12AQHHKuO2WNtWjw/article-cover_image-shrink_720_1280/0/1701050983933?e=2147483647&v=beta&t=XusrofmKvDGCfr5dUxmVFYhrojzml9t_yQ8L0WrTxOs

Example A:
High-performance analytics

Example B:
A high-performing team

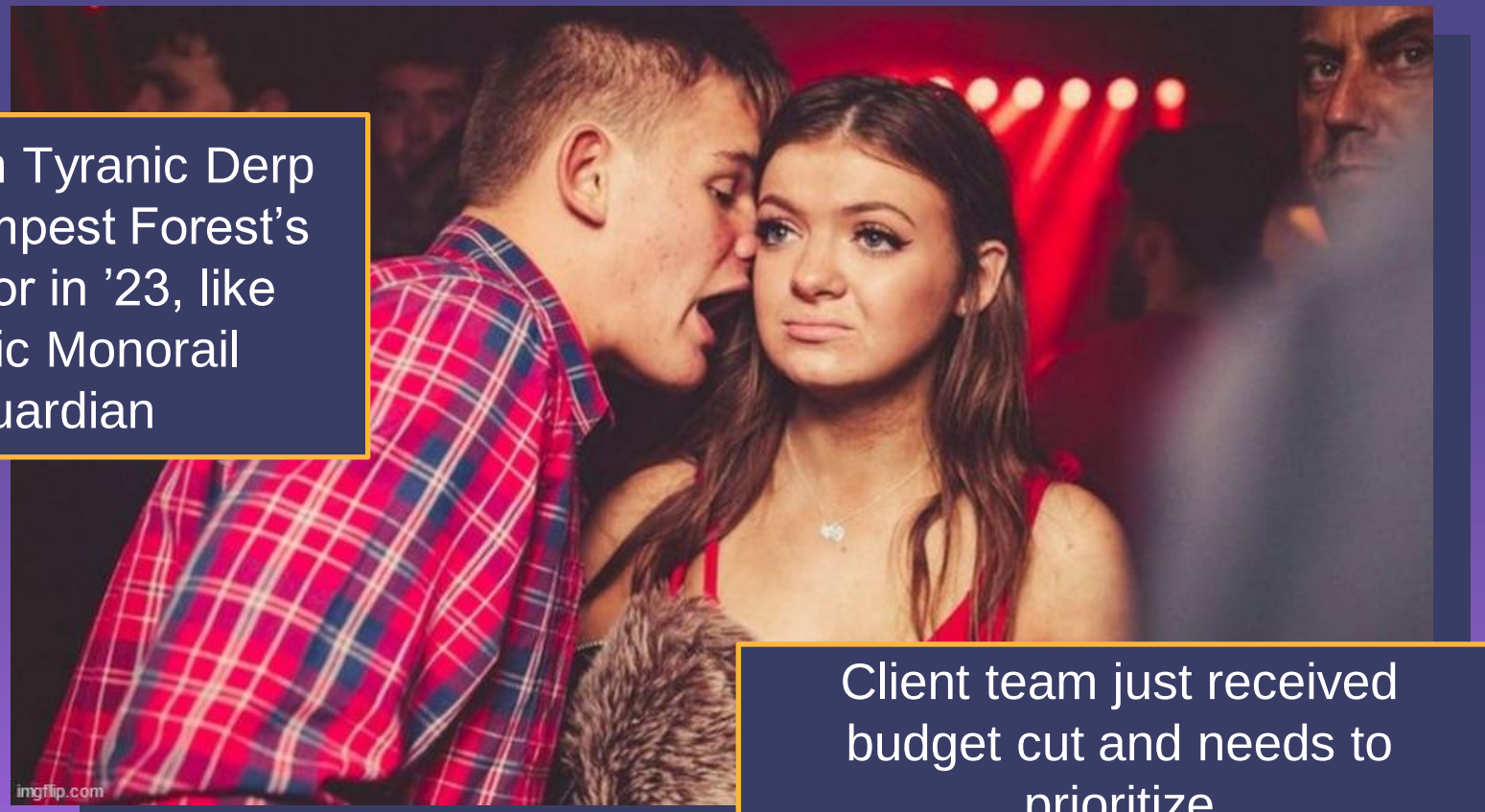
CTI context: the market



Source: https://noeticcyber.com/wp-content/uploads/Figure_1_Hype_Cycle_for_Security_Operations_2023.png

CTI context: demonstrating value as client facing team remains hard

Suburban Tyranic Derp used Tempest Forest's backdoor in '23, like Aquatic Monorail Guardian



Client team just received budget cut and needs to prioritize

Source: https://imgflip.com

CTI context: demonstrating value as onsite team also remains hard

Source: https://static.independent.co.uk/2021/07/23/15/iStock-660013672.jpg

Building a (cyber threat intelligence) team in this context

Input

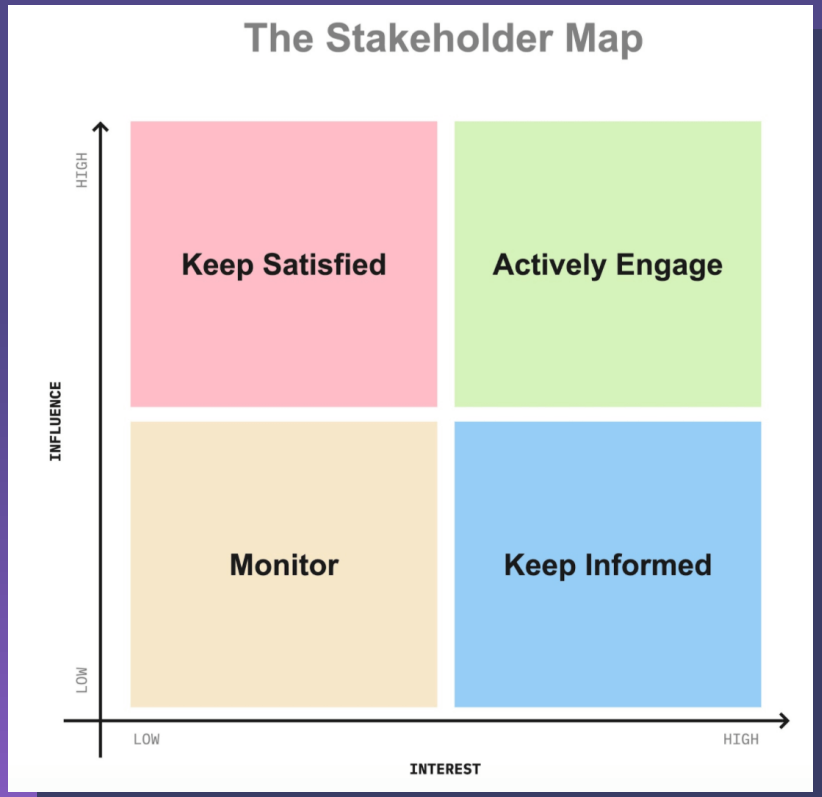
Process

result

Recipes

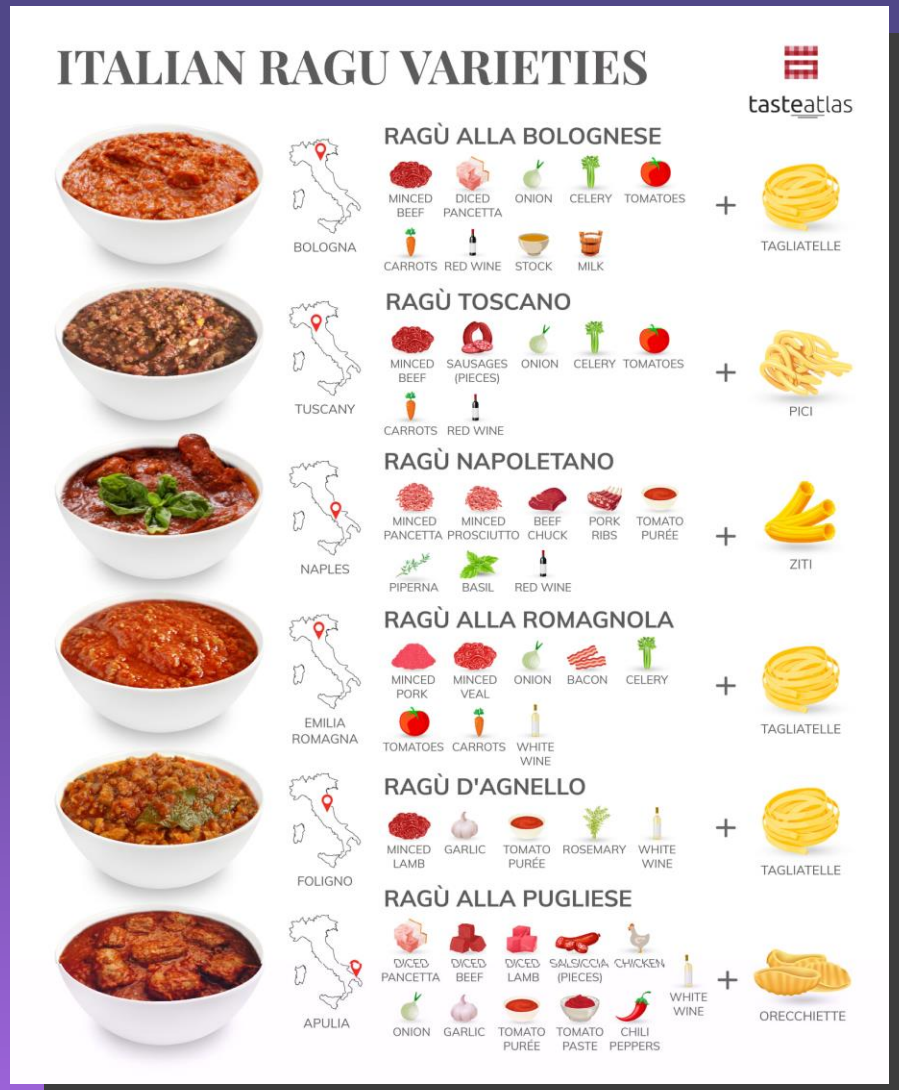
Get to know your eaters

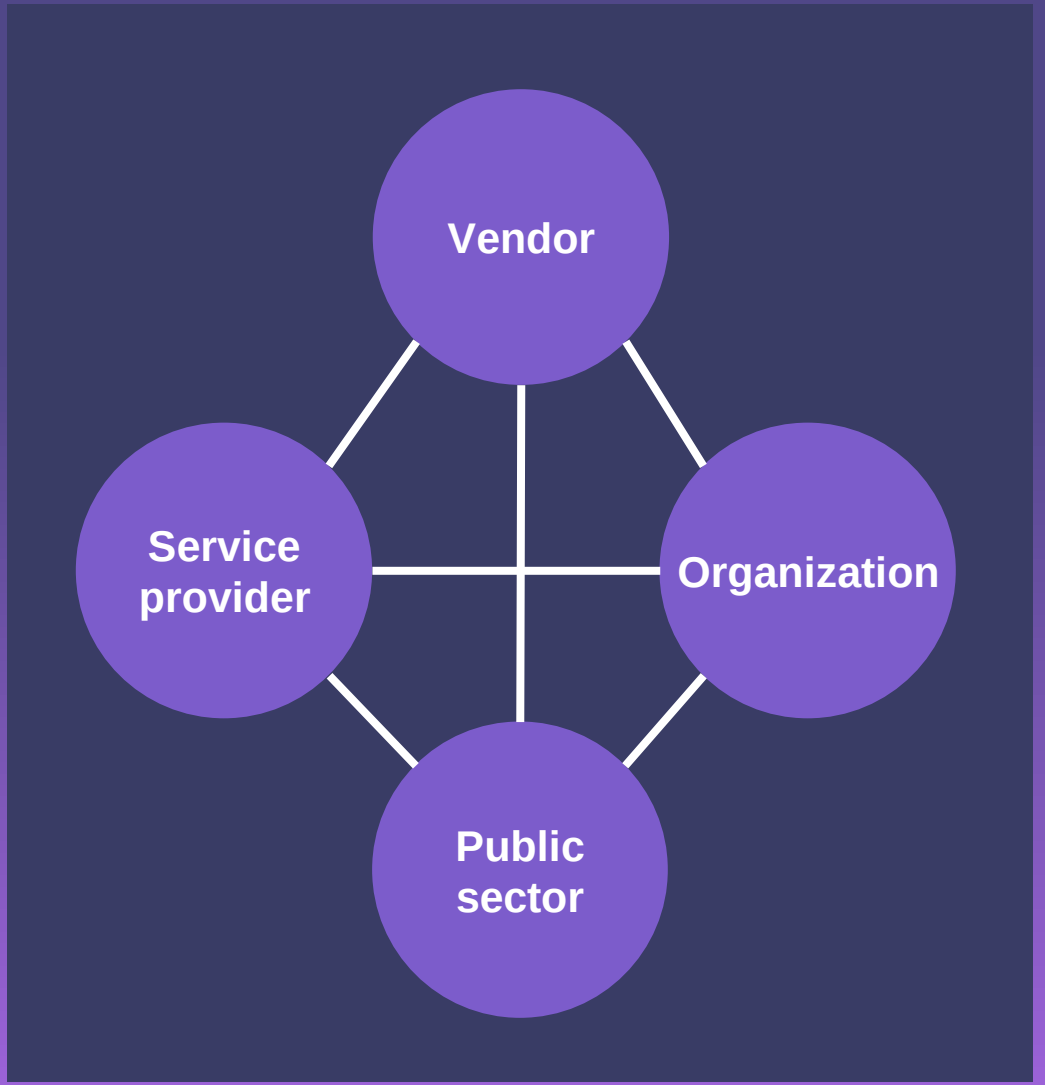
Source:
https://cdn.shopify.com/s/files/1/0540/7757/products/Mess_when_toddler_eating_large.jpg?v=1471784101



Source:
https://www.pendo.io/pendo-blog/wp-content/uploads/sites/3/2020/08/stakeholder-map.png

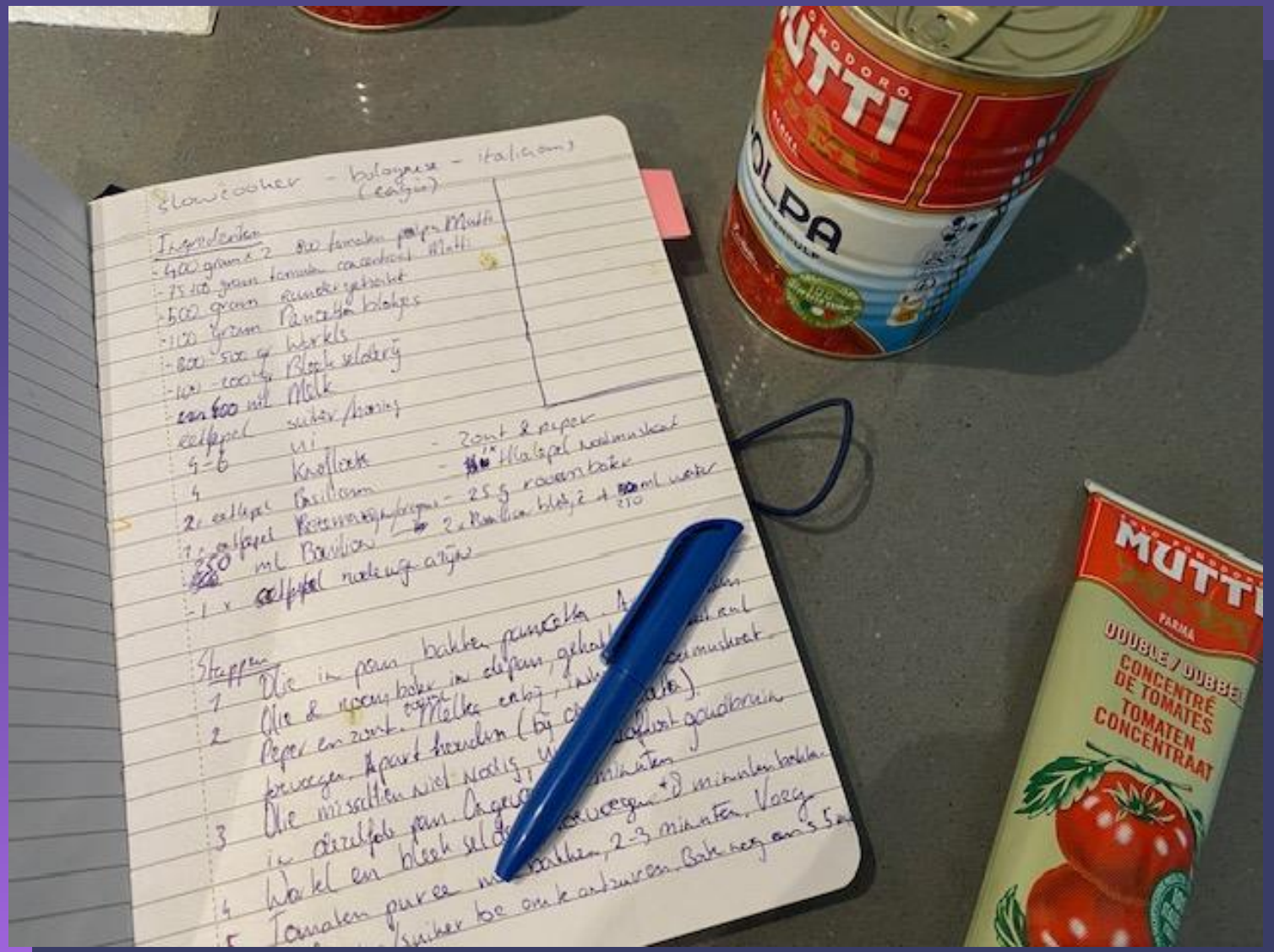
Recipes for specific types of organizations



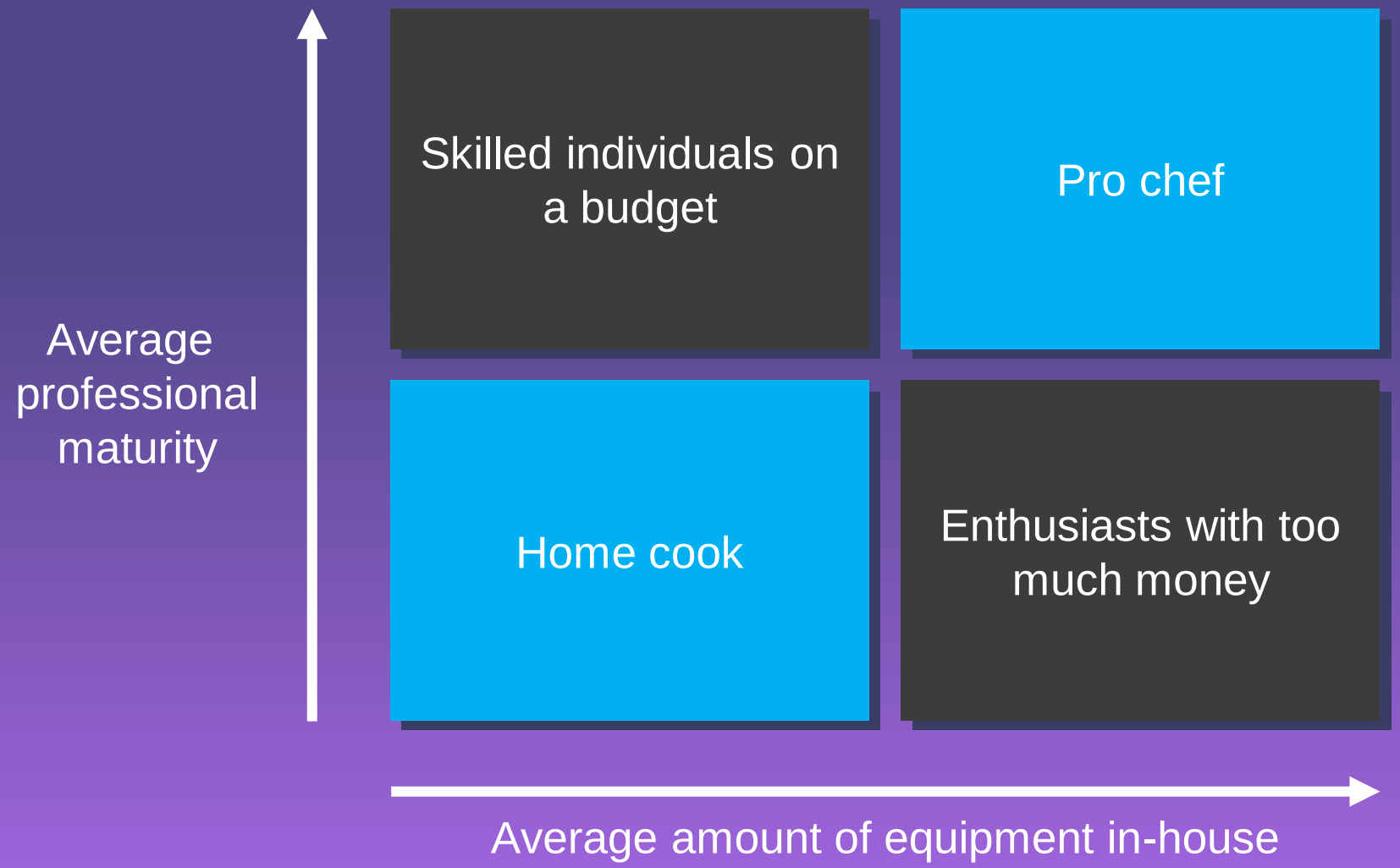


Source: https://scontent-ams2-1.xx.fbcdn.net/v/t1.6435-9/200597721_2992056704363346_5258724624925645000_n.jpg?_nc_cat=106&ccb=1-7&_nc_sid=dd63ad&_nc_ohc=d_5bXgLdgY0AX-Pw_qh&_nc_ht=scontent-ams2-1.xx&oh=00_AfDTe3nBLHsG14t0ffVQkgfttUnGFPQF0s6NZUb-prB2w&oe=65CF42B9

Cooking books & honing your process



Cooking equipment



Key ingredients to be(come) high performing

Culture: It takes time to build

Source: https://imgflip.com/i/8crkda

Team: Creating your ‘esprit de corps’

Viewer tip

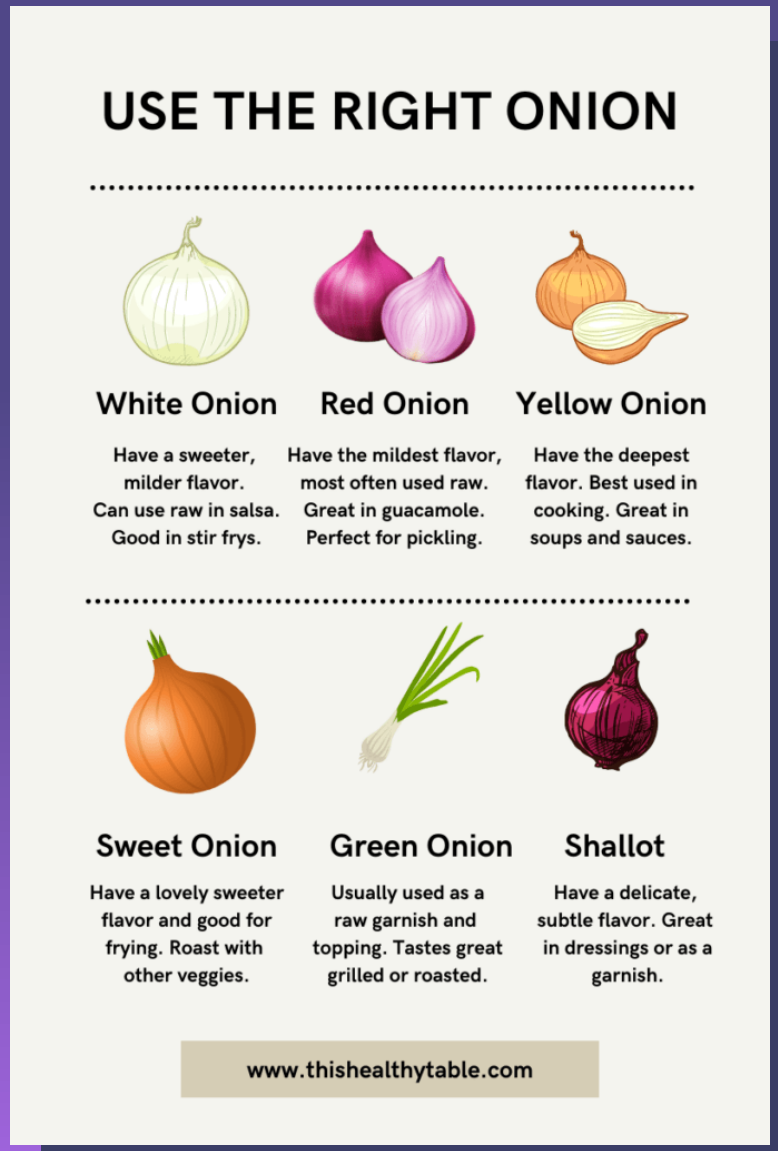
Track One

Sharing, Compared: A Study on the Changing Landscape of CTI Networking

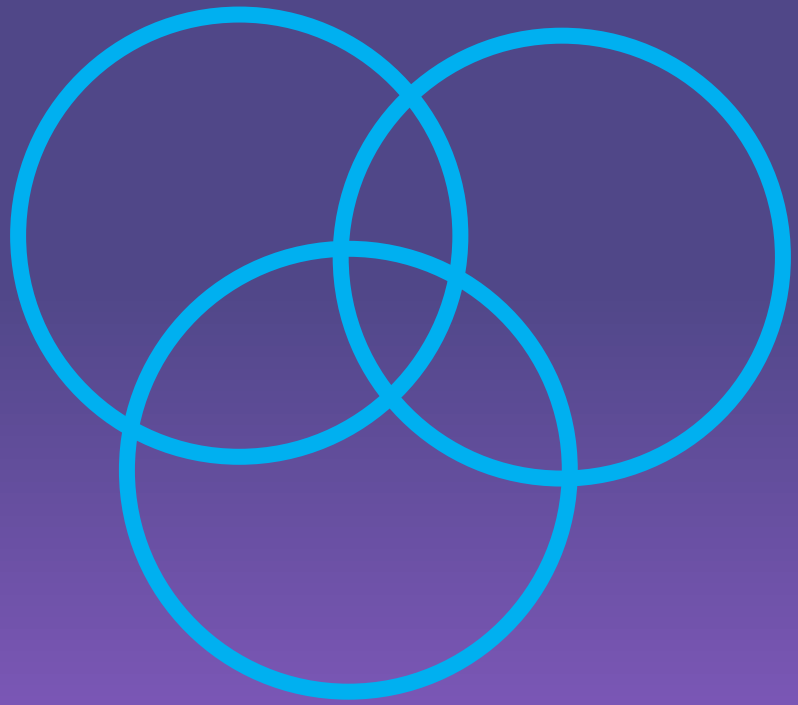
Grace Chi, Co-Founder & COO, Pulsedive

Show More

Team member:



Source: https://thishealthytable.com/blog/types-onions/



Overlaps in personality, skills or other is dictated by ambition, purpose and objectives of the team

Embracing the corporate grand mothers

Source:
https://media.istockphoto.com/id/820628874/photo/grandma-looking-at-her-granddaughter.jpg?s=612x612&w=0&k=20&c=TF7RQcoMuRqkebAyO54VrjIE-N3F0f-_L3kA61w4dlg=

On leadership

Source:
https://i0.wp.com/thekeysmashblog.com/wp-content/uploads/2023/06/The-Menu.png?resize=825%2C464&ssl=1

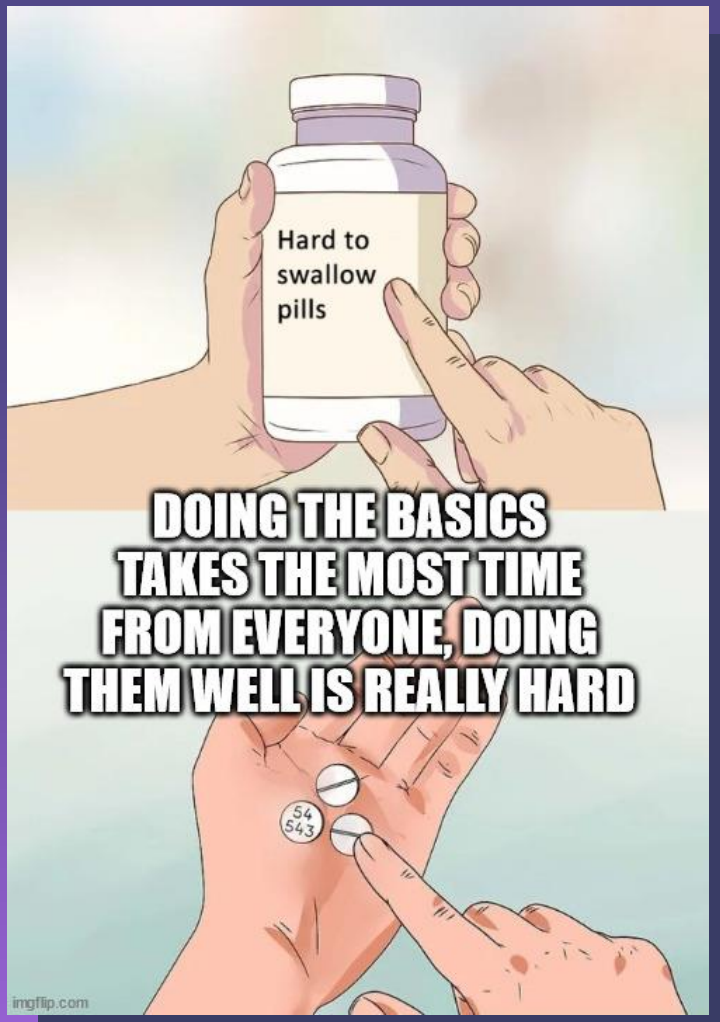
- Positional
- Intentional
- Authentic

Leadership

Especially relevant within the CTI space

Cooking

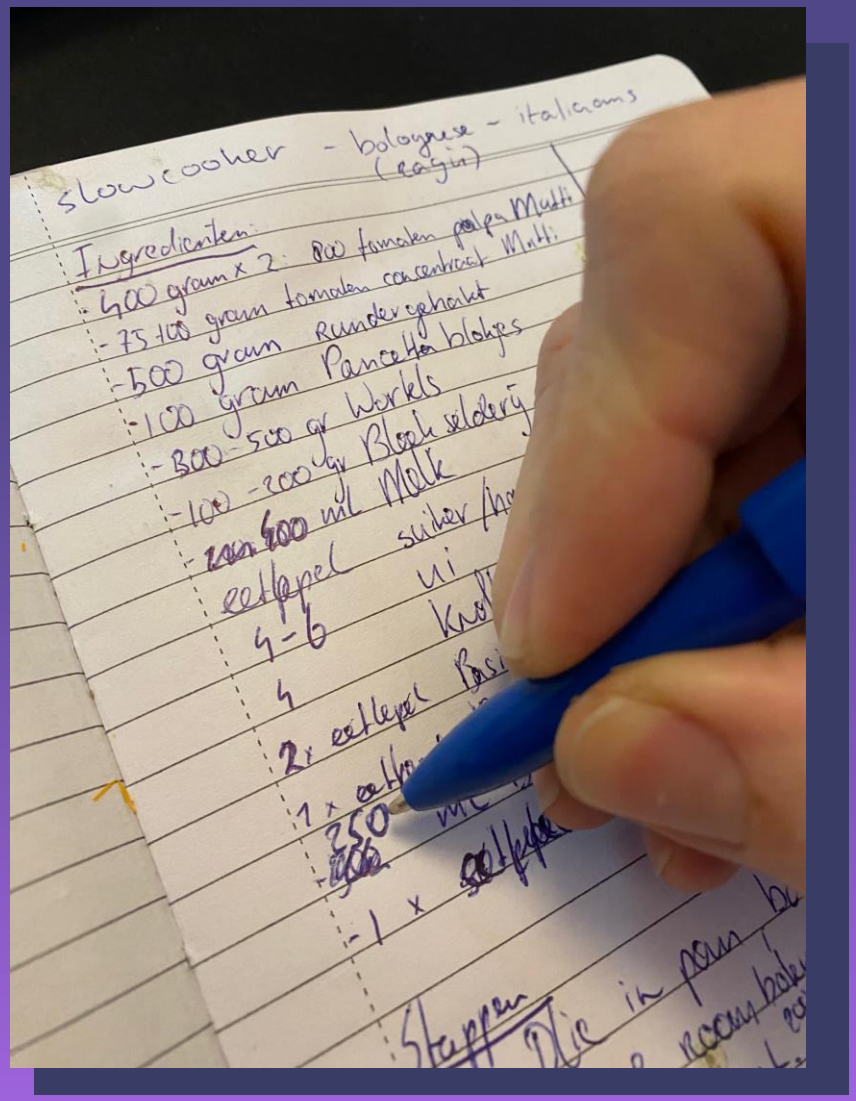
Mindset: sweat the ‘mise en place’



Source: https://imgflip.com/i/8crgc2

On embracing failure

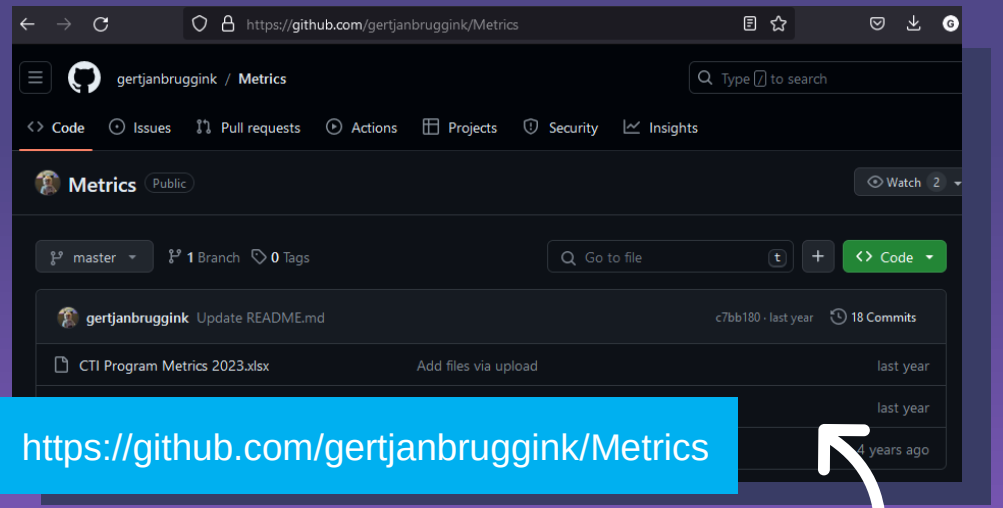
Growth of you, your team and your culture



Nonlinear thinking
Embracing complexity, randomness, and ambiguity, often exploring multiple possibilities and embracing interconnectedness ideas

CTI specific

Comparing & measuring



https://github.com/gertjanbruggink/Metrics

One example, there are plenty

Demonstrating value

Client Example:

A story on leveraging stakeholder engagement to delivery short term results and build long-term relationships.

Wrapping it up

My Ragu' alla bolognese recipe

Ingredients:
- 800 gram / 28 Oz Tomato sauce
- 75-100 gram / 2.6-3.5 Oz Tomato paste
- 500 gram / 17 Oz minced meat
- 100 gram /3.5 oz pancetta blocks
- 500 gram / 17 Oz Carrots
- 100-200 gram / 3.5-7 Oz Celery
- 400 ML Milk
- 25 gr / 0.8 Oz butter
- Spoon honey or sugar
- 4-6 Onions
- 4 Garlic toes
- 1 tablespoon Basil
- 1 tablespoon Rosemary
- 1 teaspoon Nutmeg
- 250 ML / broth, using 2 broth cubes
- 2 tablespoon Red wine vinegar
- Salt & pepper, on taste
- Cooking oil at the ready
- Spaghetti or tagliatelle based on number of eaters

Equipment :
- Slow cooker
- Frying pan
- Cutting boards
- Knives
- Spatula
- Peeling equipment
- Patience

Steps:
1. Cut onions, garlic, carrot & celery in small pieces. Make sure to properly peel the celery, preventing long strings to remain.
2. Cooking oil in pan, fry Pancetta. Once baked, keep separate. You can do this in your slow cooking pan if its stove resistant.
3. Add a bit more oil and the butter to the pan. Put the minced meat in. Season with Salt, pepper and nutmeg. Once sufficiently fried, add 200 ML of milk and let it fry until the meat has absorbed the milk. Keep separate when ready.
4. Oil might not be needed in the pan, as probably much is left from the meat; fruit onions on very low temperature until they are golden brown. This takes like 8-10 minutes. After 5 minutes add the garlic.
5. Add the cut carrots and celery. Fry together around 8 minutes.
6. Add tomato paste. Give it a good stir. Fry for around 3 minutes. Afterwards, add spoon honey (or sugar) to reduce the acidity. Fry for another 5 minutes.
7. Add the dried herbs. Fry for 2 minutes.
8. Add the broth, tomato sauce, the remaining milk (200ML) and red wine vinegar. Stir properly.
9. Add the minced meat and pancetta. Again, stir properly.
10. Move everything into the slow cooker: 6-8 hours on the lowest setting or 4-6 hours on the highest setting.
11. Ground rules: the longer the better; it's even better when eating it the next day.

Considerations
- Number of eaters: 4. If you cook for around 8, recommend don't doubling the ingredients but increase ingredients by ~50%.
- I tend to fry both Pancetta and Minced meat in a separate pan. This way I can fry the vegetables in the slow cooker.
- Use quality tomato sauce; higher quality is less acidic.
- I use red wine vinegar instead of red wine because I have kids and they don't need alcohol.
- Based on feedback I started reducing the amount of broth because the kids found it too moist. If you eat the ragu the next day you don't have that issue, except my kids don't have that patience.

My team recipe

Ingredients:

Steps:

1. It’s never only about content, it’s always about people.
2. Start thinking non-linear about CTI team ingredients (the team, its members, or the leadership).
3. A continuous improvement mindset get’s you to 80%. The remainder is sheer ambition and grit.

Source: https://www.lego.com/en-us/kids/sets/minifigures/series-18-party-a9666914412343c489d153022eeb7c25

Thanks folks! 👋

Practitioner & hands-on client support in

- Cyber Threat Intelligence
- Risk Management
- Capability Building
- Intelligence-led Red Teaming
- Transformation Programs
- Strategic Change

Most notably in these industries

- Financial Services
- High Tech
- Manufacturing

Rest of my time goes into

- Entrepreneurship
- Coaching
- Volunteering
- Research
- Father x 2
- Gaming
- Lego
- Meme's
- Sports

Gert-Jan Bruggink

Cyber threat cartographer
CTI Bob Ross
Cyber weatherman
Lego afficionado

@gertjanbruggink
github.com/gertjanbruggink
/gertjanbruggink