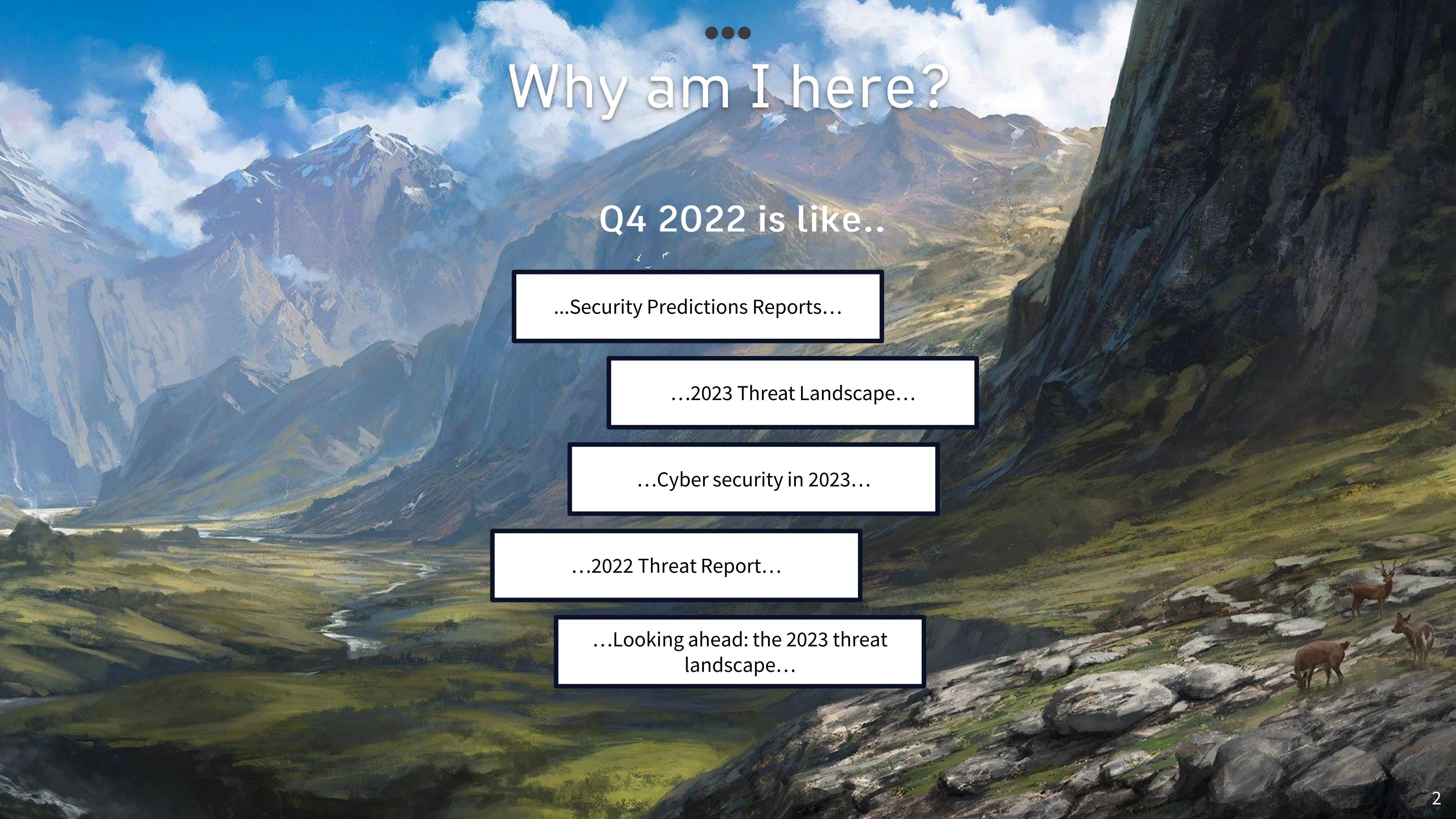
The Joy of Threat Landscaping

By Gert-Jan Bruggink

FIRST CTI Summit 2022

2 November 2022

Why am I here?



Q4 2022 is like..

...Security Predictions Reports…

…2023 Threat Landscape…

…Cyber security in 2023…

…2022 Threat Report…

…Looking ahead: the 2023 threat landscape…

Hi there! 👋

Cyber Threat Intelligence | Risk Management | Capability Building

Intelligence-led Red Teaming | Transformation Programs | Strategic Change

Financial Services | High Tech | Manufacturing

Volunteering | Coaching | Entrepreneurship | Research

Father x 2 | Gaming | Painting | Lego | Meme’s

Gert-Jan Bruggink

cyber threat cartographer

&

founder Venation

@gertjanbruggink
github.com/gertjanbruggink
/gertjanbruggink

What am I going to talk about?

✓ What is this so-called threat landscape?

✓ How do you produce such a thing?

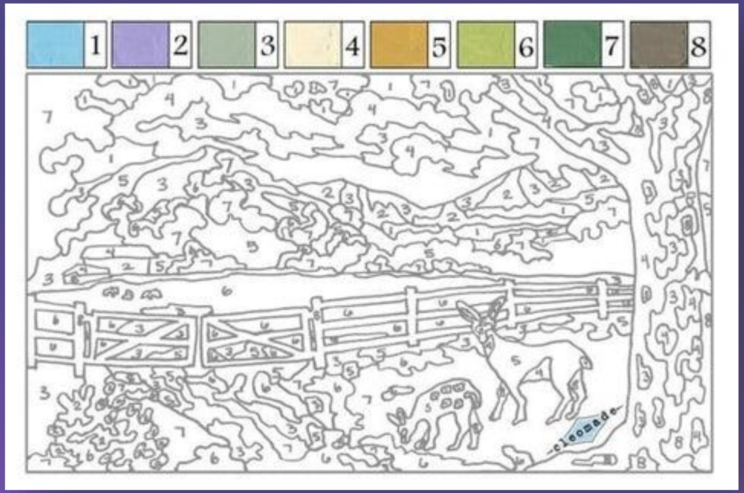
✓ Dos and don’ts

Objective: enabling professionals to build proper threat landscape deliverables by themselves

The ‘threat landscape’ deliverable

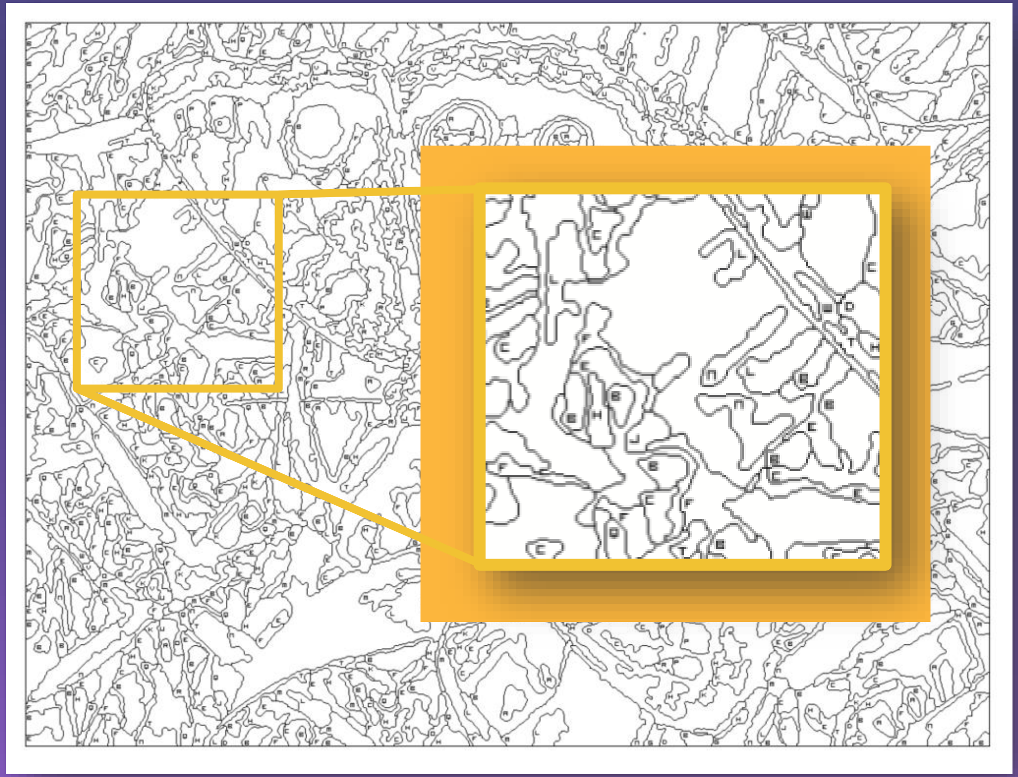
Public sector vs private sector applications

Private



Source: https://paintingbynumbersshop.com/blogs/blog/paint-by-numbers-what-is-it

Public



Source: https://paintbynumberspro.com/printable-painting-by-numbers/

What is a threat landscape

- What do people think it is?
- What do people ask for?

Source: https://www.youtube.com/watch?v=NcVeRlPu_5w

Three (main) types of threat landscapes*

Requirement based

(typically, internal)

Source: https://artkatalog.eu/en/news/49_How-to-do-Painting-by-Numbers-.html

Research based

(typically, vendors or public agencies)

Source: Learntoart.com

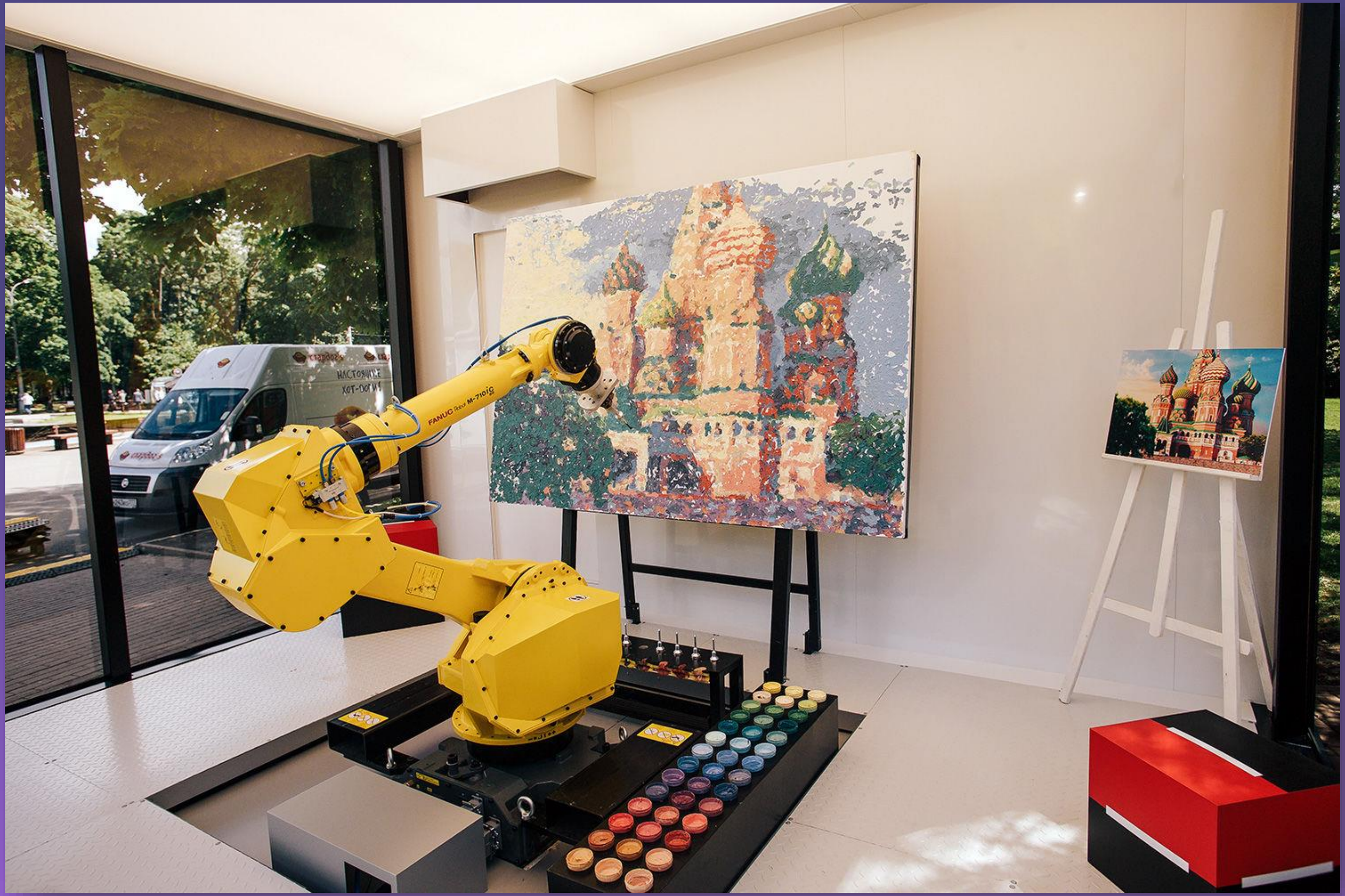
Guesstimate

(just doing what you think is right)

Source: https://pixels.com/featured/flowers-abound-abstract-yolo-art-studio.html

*in the private sector

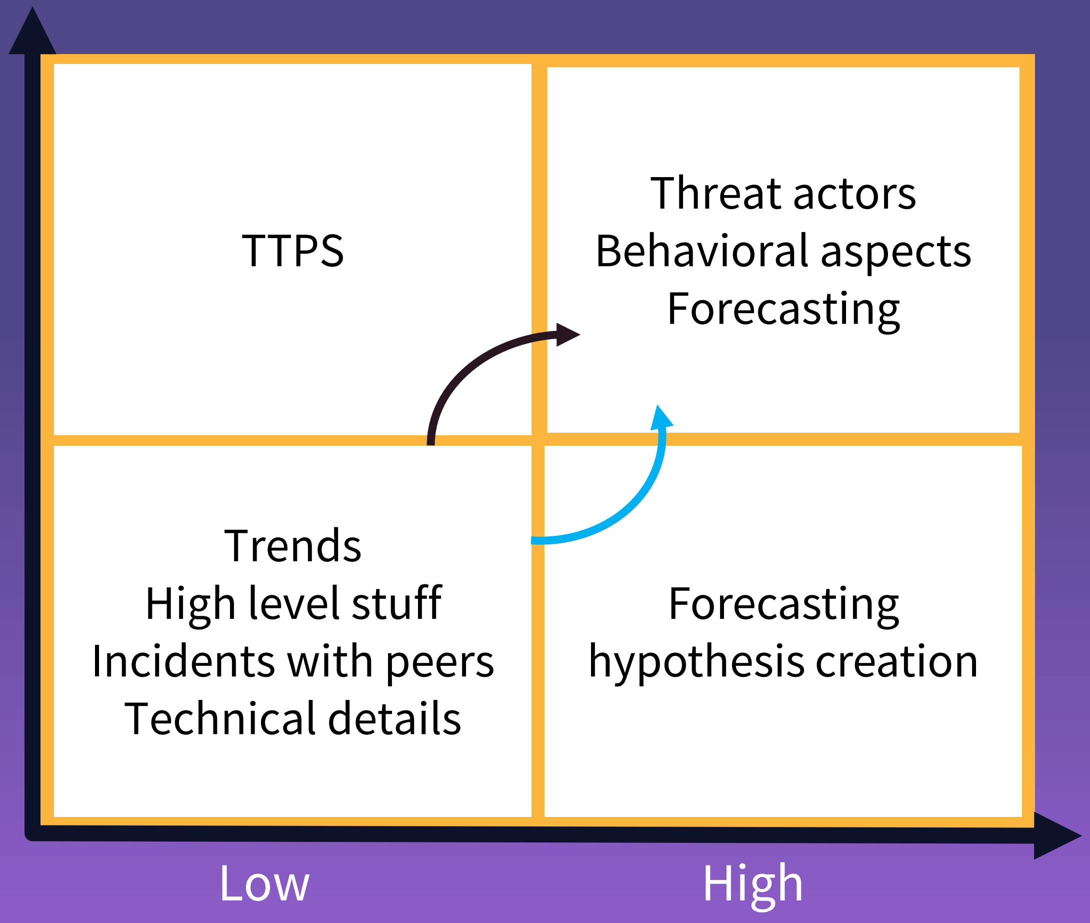
Humans' vs ‘AI’



Source: https://www.digitalartsonline.co.uk/features/illustration/this-robot-thinks-it-can-paint-it-can/

Understanding needs

Specifics



	Low	High
High	TTPS	Threat actors Behavioral aspects Forecasting
Low	Trends High level stuff Incidents with peers Technical details	Forecasting hypothesis creation

Capability of Team

Understanding of Risk

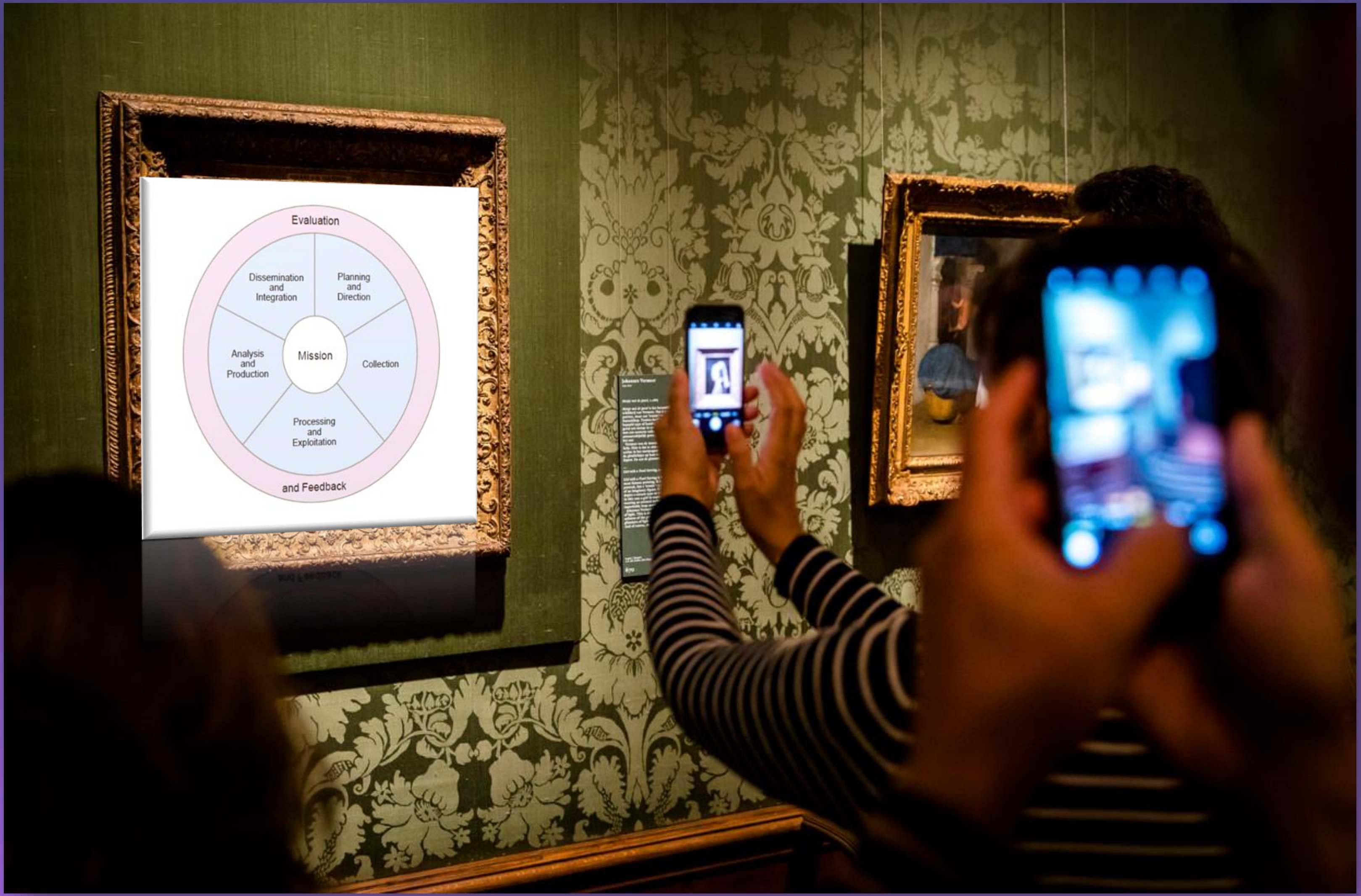
Broad strokes

Why a threat landscape

https://awe401.medium.com/think-you-dont-understand-art-think-again-a-second-perspective-b938fb9c5497

Producing the product

Process you will follow intuitively



Source: https://www.trouw.nl/nieuws/alle-schilderijen-van-vermeer-zijn-nu-toch-bij-elkaar-in-je-broekzak~b32ad718/?referrer=https%3A%2F%2Fwww.google.com%2F

Applying the process

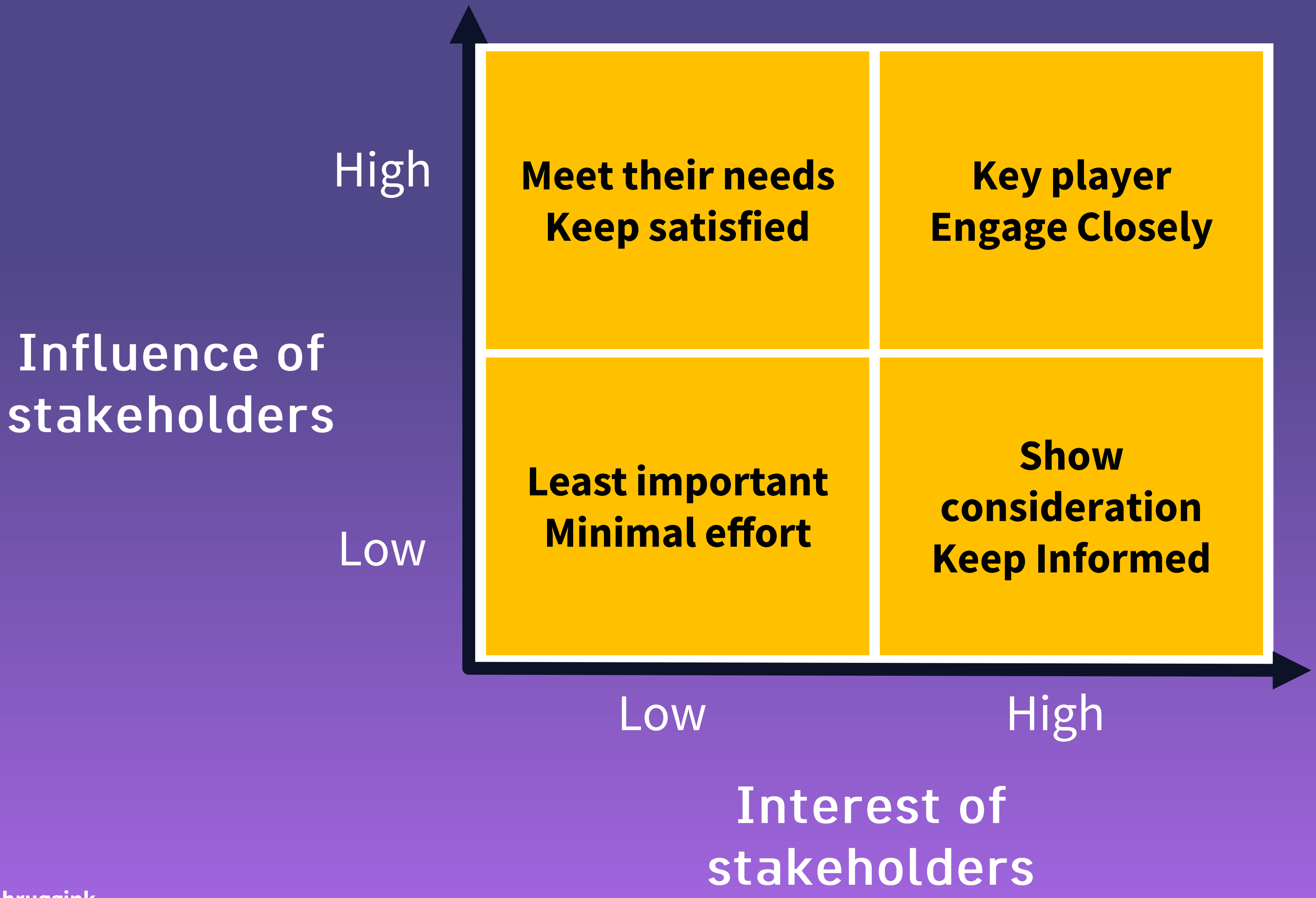
Intelligence requirements

Collection & Analysis

Dissemination

Source: https://images.collection.cooperhewitt.org/327669_659cf280d8bef871_b.jpg

Understanding your stakeholders



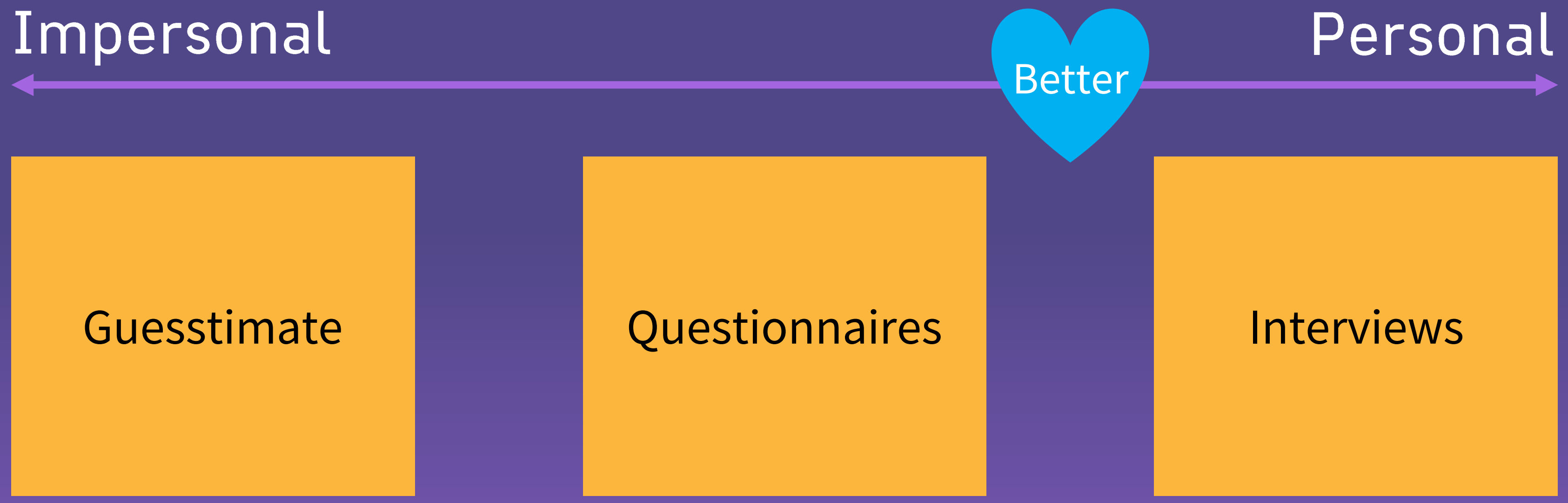
Influence of stakeholders

	Low	High
High	**Meet their needs** **Keep satisfied**	**Key player** **Engage Closely**
Low	**Least important** **Minimal effort**	**Show consideration** **Keep Informed**

Interest of stakeholders

Pro tip 💯
A consultative sales approach might be needed to engage stakeholders, educating on the value add of CTI.

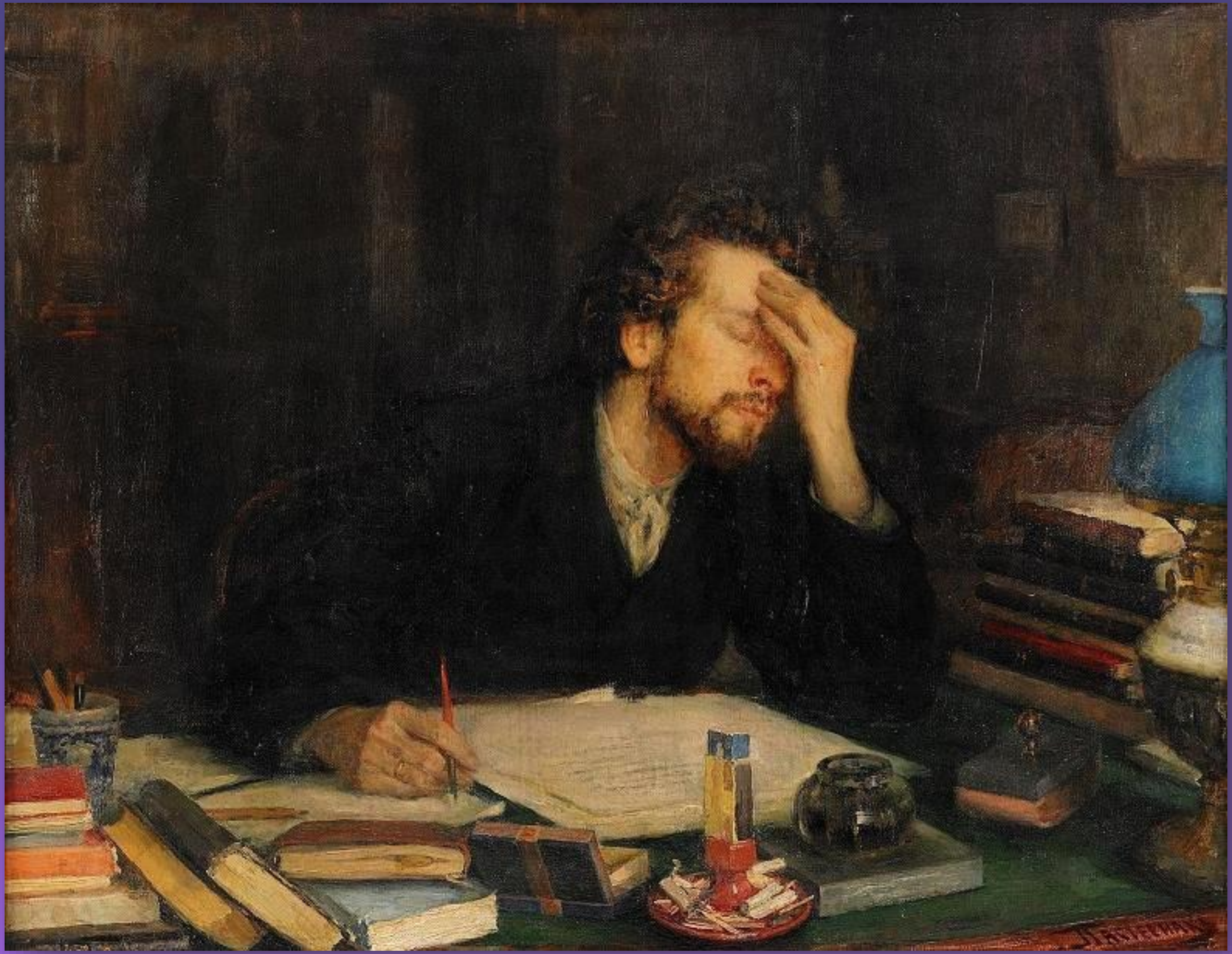
Soliciting (intelligence) requirements



Pro tip 💯

Interview stakeholders,
send them a questionnaire in advance and
discuss wants/needs afterwards.

Designing the deliverable



Source: https://commons.wikimedia.org/wiki/File:Leonid_Pasternak_-_The_Passion_of_creation_%281%29.jpg

Collection & processing

Source: https://www.bobross.com/bob-ross-master-set/

Analysis & producing the deliverable

Source: https://www.flickr.com/photos/wvs/3079565592/

Dissemination

Source: https://www.artdex.com/wp-content/uploads/2021/12/image3-768x512.jpg

Feedback, or a word on improving

- Experiment!
- Peer review regularly.
- Improve iteratively.

ImGonnaGoHome 16 points · 17 hours ago
Yeah, well, he's got a cat now. That counts for something, right?

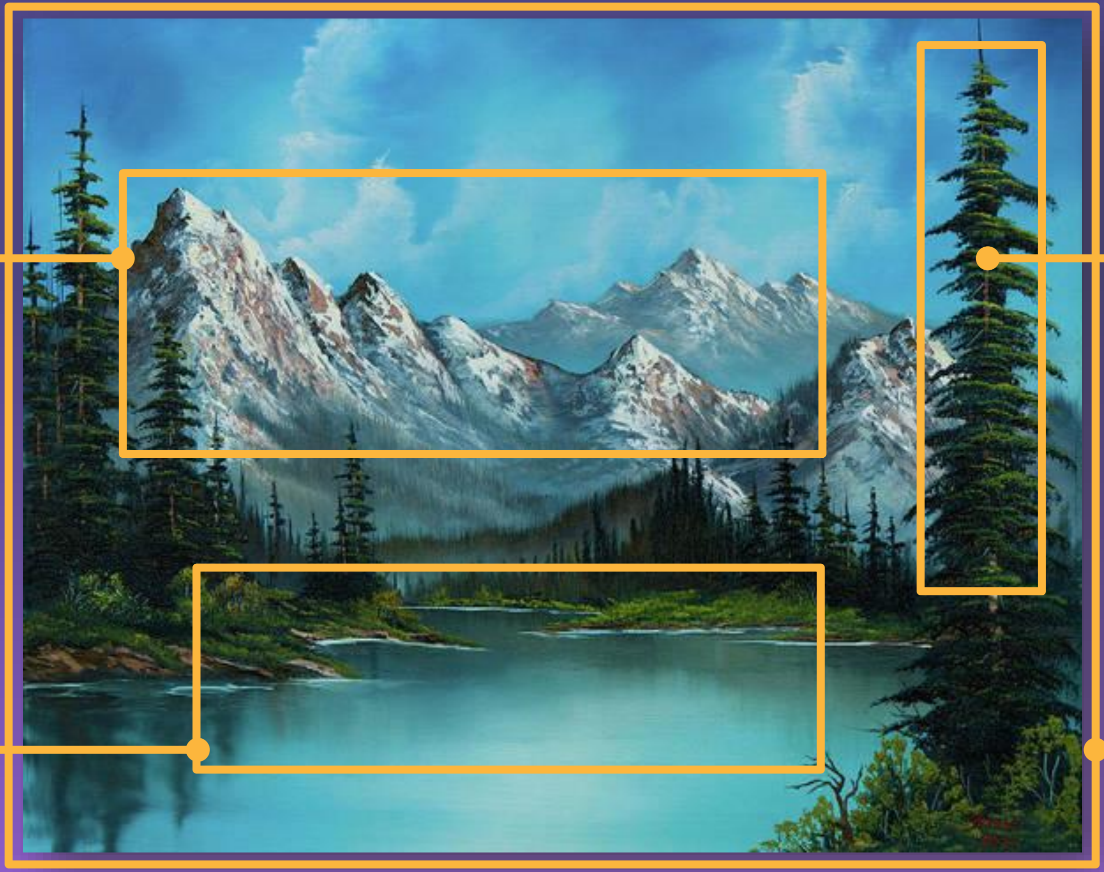
DonaldIgwebuike 12 points · 15 hours ago
I will bet you a dollar we see that cat in a painting soon.

1 more reply

Source: https://www.reddit.com/r/pics/comments/ht0dld/i_painted_a_self_portrait_painting_myself_oil_on/

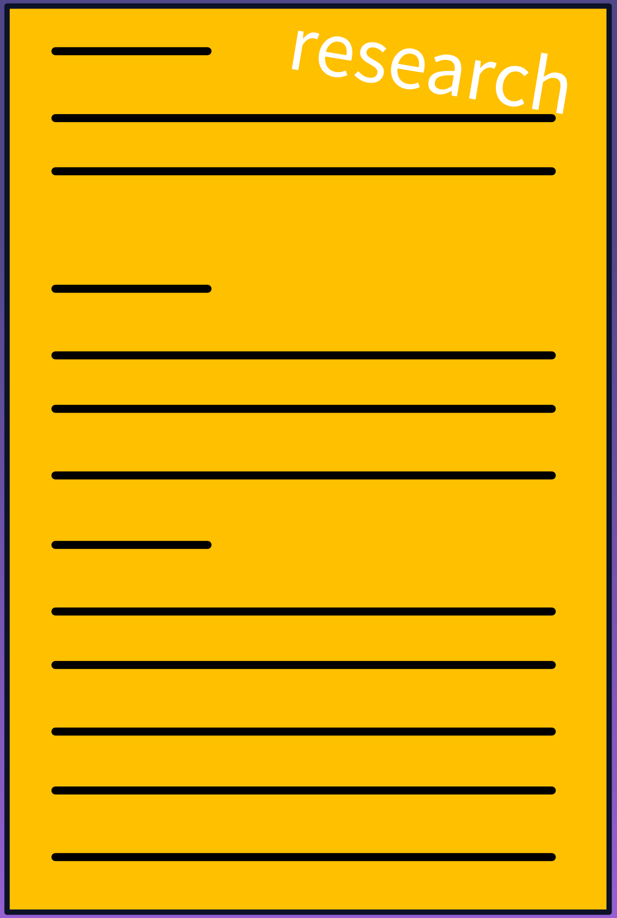
Key pointers when producing the deliverable

#1 Choosing the right format



Source: https://fineartamerica.com/featured/natures-grandeur-chris-steele.html?product=art-print

#2 Take your time designing your product



Your research

Your product

Source: https://www.youtube.com/watch?v=xdclcGGm-Yo

Overall

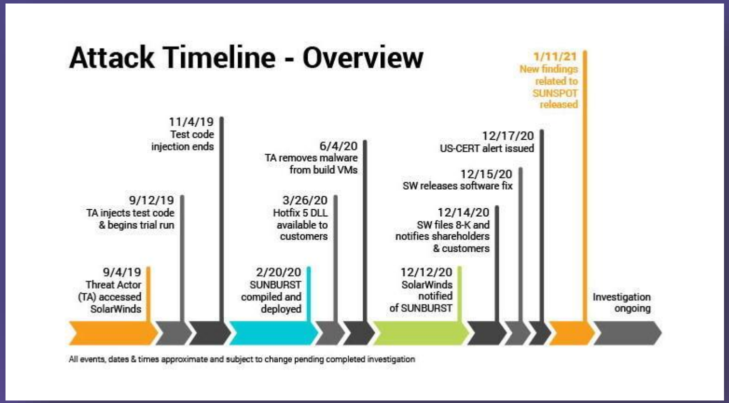
- Consider # of pages
- Less is more

Chapters

- Intelligence requirements vs. document structure
- Consider the audience

#3 Successful uses of visualizations

Timelines



Attack Timeline - Overview

9/4/19 Threat Actor (TA) accessed SolarWinds

9/12/19 TA injects test code & begins trial run

11/4/19 Test code injection ends

2/20/20 SUNBURST compiled and deployed

3/26/20 Hotfix 5 DLL available to customers

6/4/20 TA removes malware from build VMs

12/12/20 SolarWinds notified of SUNBURST

12/14/20 SW files 8-K and notifies shareholders & customers

12/15/20 SW releases software fix

12/17/20 US-CERT alert issued

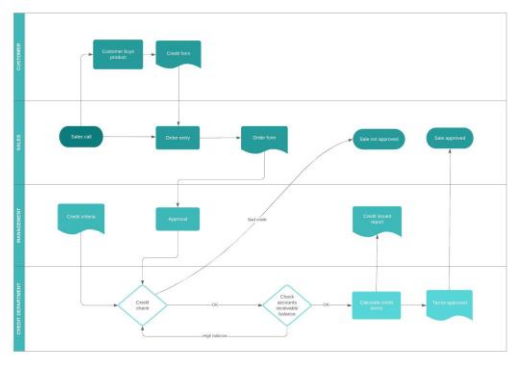
1/11/21 New findings related to SUNSPOT released

Investigation ongoing

All events, dates & times approximate and subject to change pending completed investigation

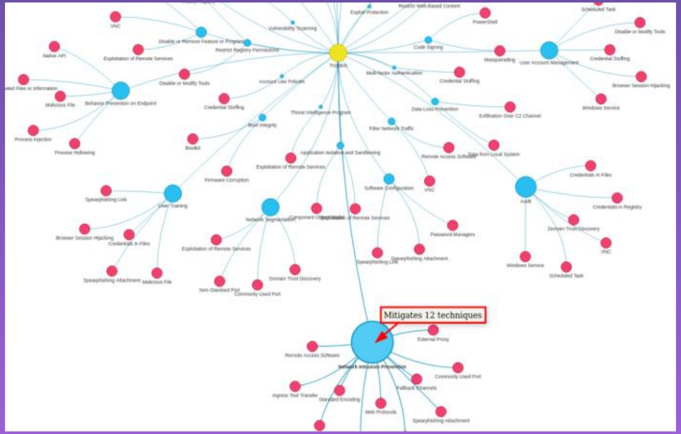
Source: https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/

Flows



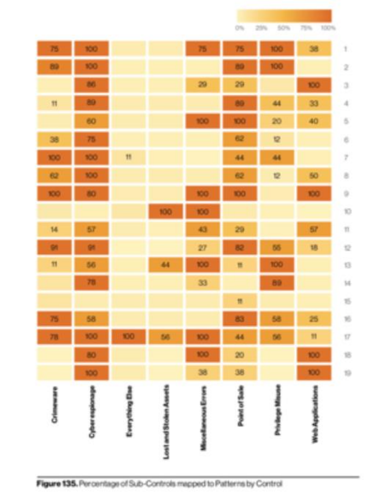
Source: https://d2slcw3kip6qmk.cloudfront.net/marketing/pages/consideration-page/Business-Process-FlowTemplate.jpeg

Relationship graphs



Source: https://media-exp1.licdn.com/dms/image/C4E12AQEX2yn12CXGsQ/article-cover_image-shrink_720_1280/0/1642458681370?e=1668643200&v=beta&t=7sq5Gs82H6Qfaz590BNYVR2gNiCNOcBSr9a2CkC5Gkc

Tables



Crimeware	Cyber espionage	Everything Else	Lost and Stolen Assets	Miscellaneous Errors	Point of Sale	Privilege Misuse	Web Applications	
75	100			75	75	100	38	1
89	100				89	100		2
	86			29	29		100	3
11	89				89	44	33	4
	60			100	100	20	40	5
38	75				62	12		6
100	100	11			44	44		7
62	100				62	12	50	8
100	80			100	100		100	9
			100	100				10
14	57			43	29		57	11
91	91			27	82	55	18	12
11	56		44	100	11	100		13
	78			33		89		14
					11			15
75	58				83	58	25	16
78	100	100	56	100	44	56	11	17
	80			100	20		100	18
	100			38	38		100	19

0% 25% 50% 75% 100%

Figure 135. Percentage of Sub-Controls mapped to Patterns by Control

Source: https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf

#4 Using assessments in your threat landscape

- In doing your analysis, you might be able to make assessments.
- When making assessments in a threat landscape, include confidence and likelihood.
- For example:

  We assess with <**insert confidence**> that <**insert assessment** - for example on **likelihood**> because of <insert **evidence**> <insert **sources**>.

Pro tip 💯
Plan a moment periodically to review & benchmark everyone's assessments: great for year-end wrap ups and proactiveness to the organization.

#5 Considering your audience

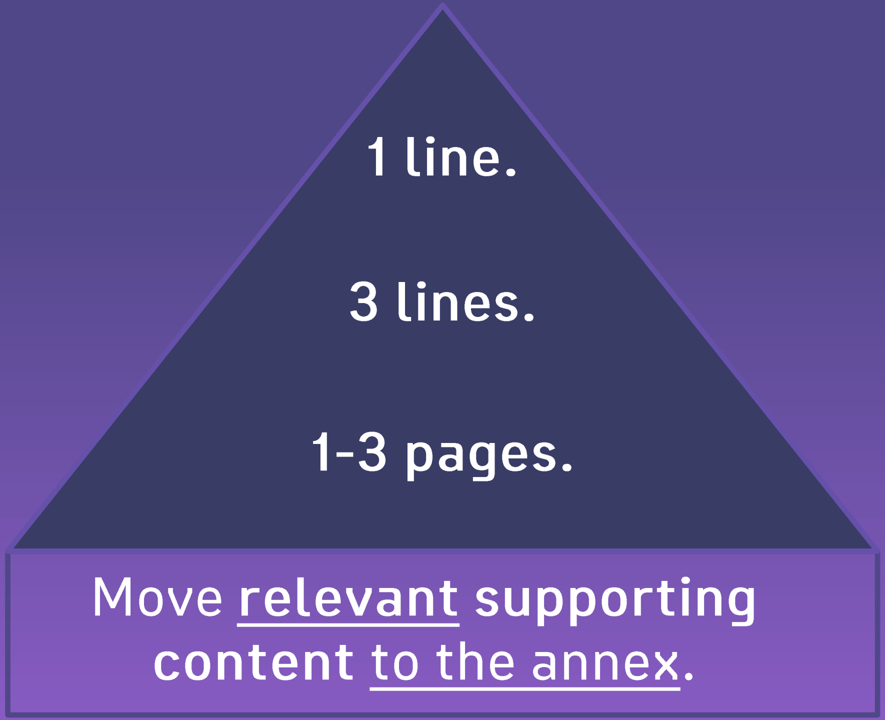
- **Decision makers** 👩‍💼
  What information is relevant for them to make decisions on?

- **Analysts** 🕵️‍♀️
  What is relevant for other analysts?

Pro tip 💯

Consider making specific chapters for each audience, to add the right levels of granularity.

#6 GJ’s ‘Bottom-Line-Up-Front’ Pyramid



1 line.

3 lines.

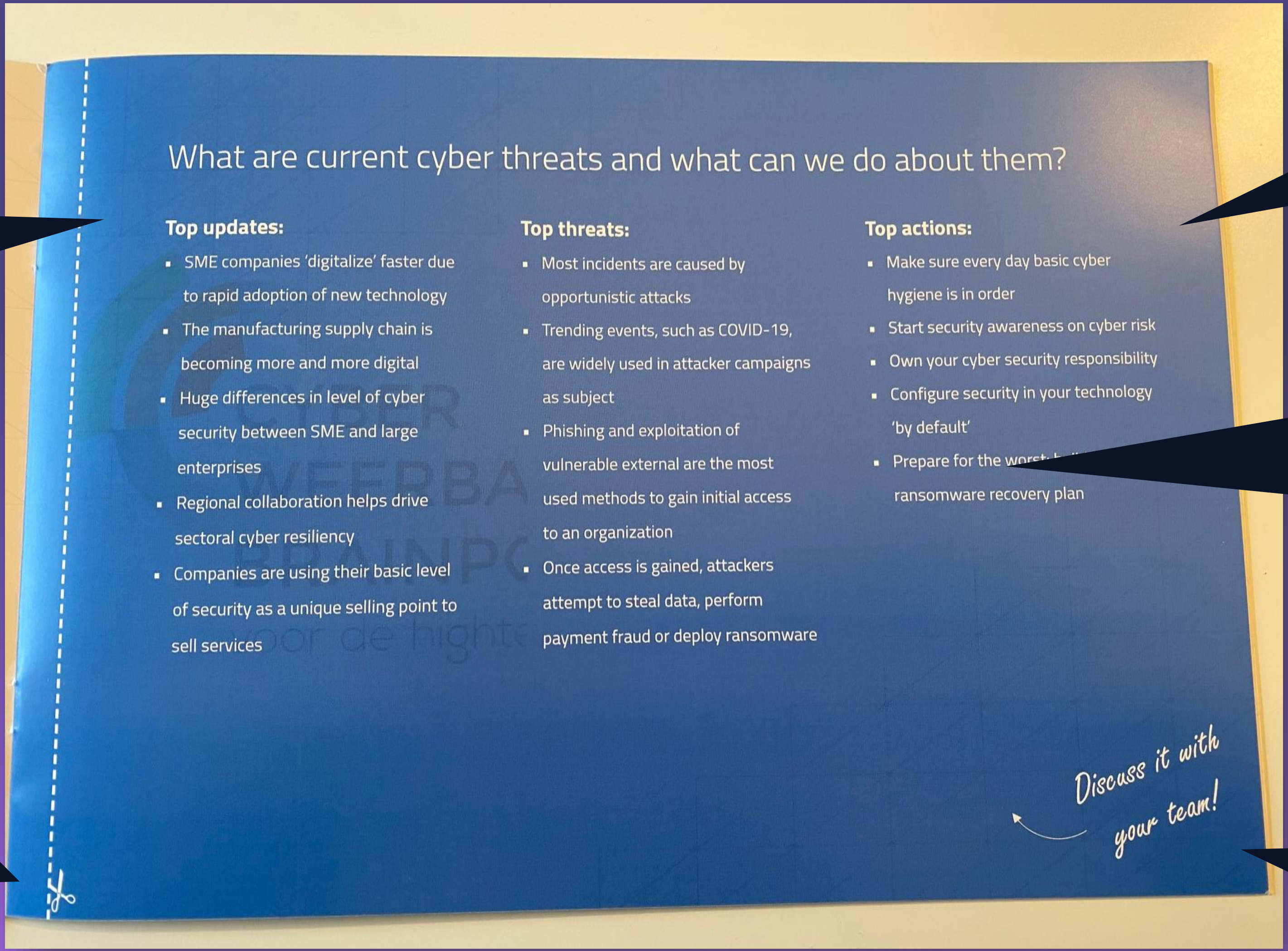
1-3 pages.

Move relevant supporting content to the annex.

Example product (summary page)

Structured based on intelligence requirements

Suggestions to cut out summary page and discuss with stakeholders



What are current cyber threats and what can we do about them?

Top updates:

- SME companies 'digitalize' faster due to rapid adoption of new technology
- The manufacturing supply chain is becoming more and more digital
- Huge differences in level of cyber security between SME and large enterprises
- Regional collaboration helps drive sectoral cyber resiliency
- Companies are using their basic level of security as a unique selling point to sell services

Top threats:

- Most incidents are caused by opportunistic attacks
- Trending events, such as COVID-19, are widely used in attacker campaigns as subject
- Phishing and exploitation of vulnerable external are the most used methods to gain initial access to an organization
- Once access is gained, attackers attempt to steal data, perform payment fraud or deploy ransomware

Top actions:

- Make sure every day basic cyber hygiene is in order
- Start security awareness on cyber risk
- Own your cyber security responsibility
- Configure security in your technology 'by default'
- Prepare for the worst ransomware recovery plan

Discuss it with your team!

Both physical and digital versions

Bullet points, active voice and to the point

Details behind this page, same structure

Source: https://cwbrainport.nl/cwb-geeft-eerste-dreigingsrapport-uit/ [2020]

Wrapping it up

Do’s and don'ts

- FUD doesn’t work. Especially in threat landscapes.
- Never exaggerate the role of APTs versus commodity cybercrime.
- Indicators of Compromise are dead. Long live Tactics, Techniques & Procedures - oh wait.

✓ Need to include details (e.g. threat actors)? Use visuals (e.g. scorecards) over long page details.

✓ Expect follow-up questions to your threat landscape and prepare accordingly.

✓ Less is more for decision makers. More is more for analysts.

Let’s continue the discussion!

Looking for more content on
building threat landscapes?

Gert-Jan Bruggink

@gertjanbruggink
/gertjanbruggink
gertjanbruggink@venation.digital
www.venation.digital