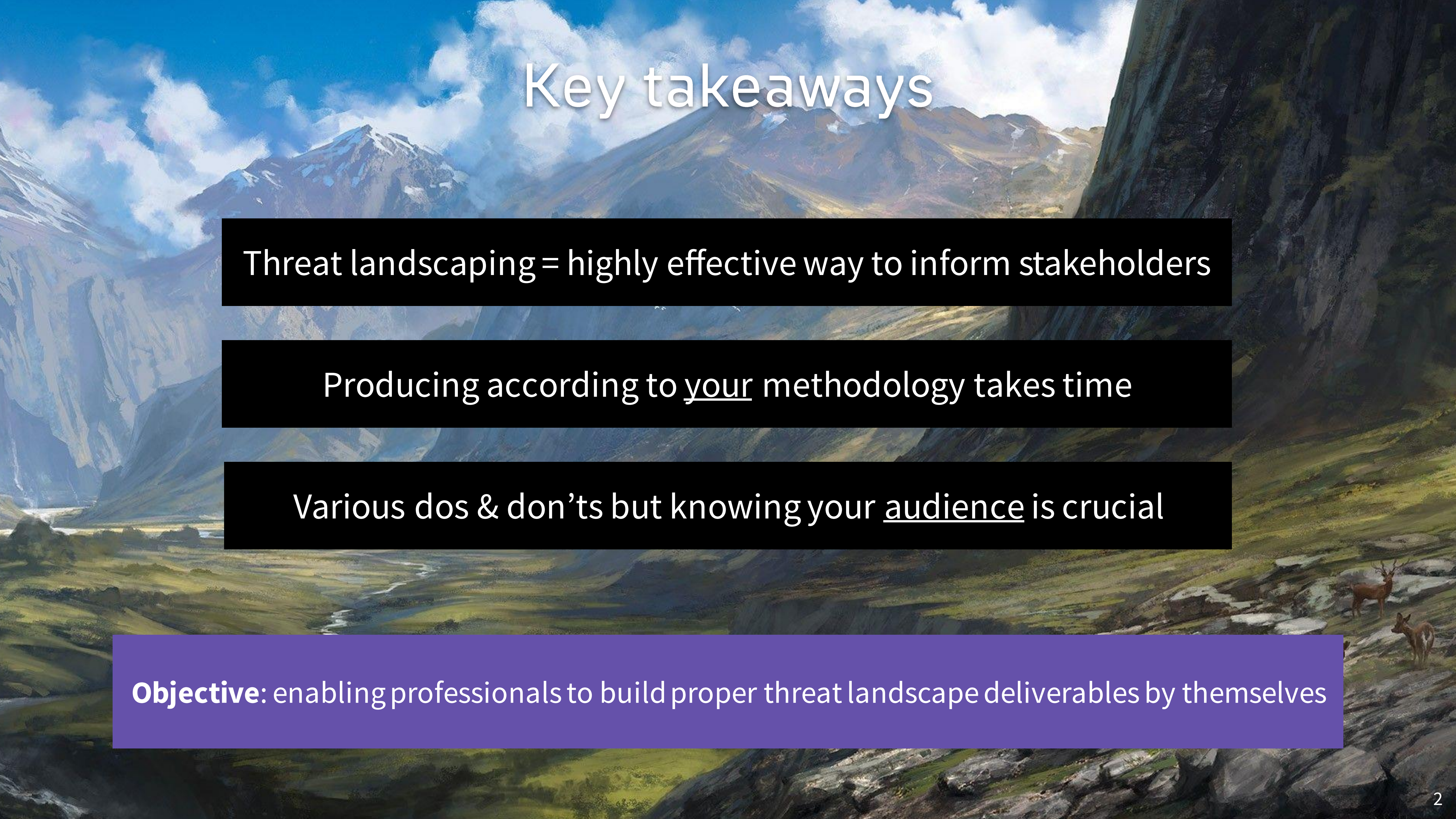
The Joy of Threat Landscaping

5 key lessons learned from applying ENISA's CTL methodology

Gert-Jan Bruggink

CTI-EU Summit 2023
13 November 2023



Key takeaways

Threat landscaping = highly effective way to inform stakeholders

Producing according to your methodology takes time

Various dos & don’ts but knowing your audience is crucial

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

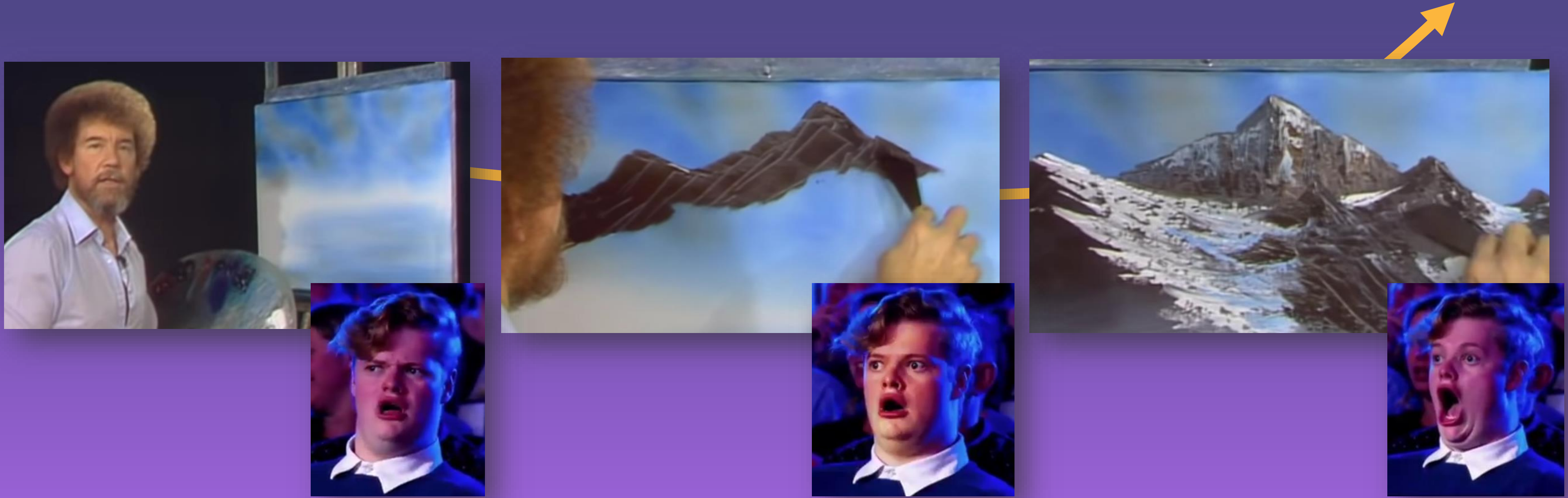
What is a threat landscape

Alternatively, why the threat landscape deliverable remains a crucial deliverable for any CTI team

enisa

ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY

JULY 2022



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

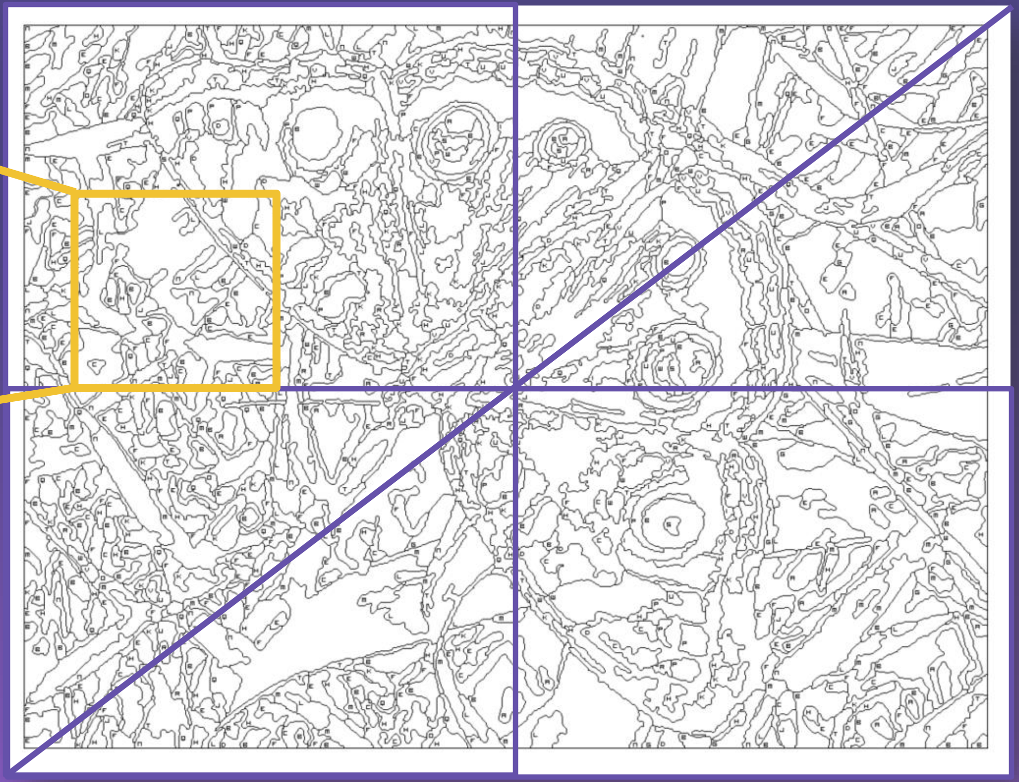
#1, Recognise the difference between types

Individual entity

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

- □ **Requirement based** (typically, internal)
- □ **Research based** (typically, vendors or public agencies)
- □ **Guesstimate** (just doing what you think is right)

ENISA

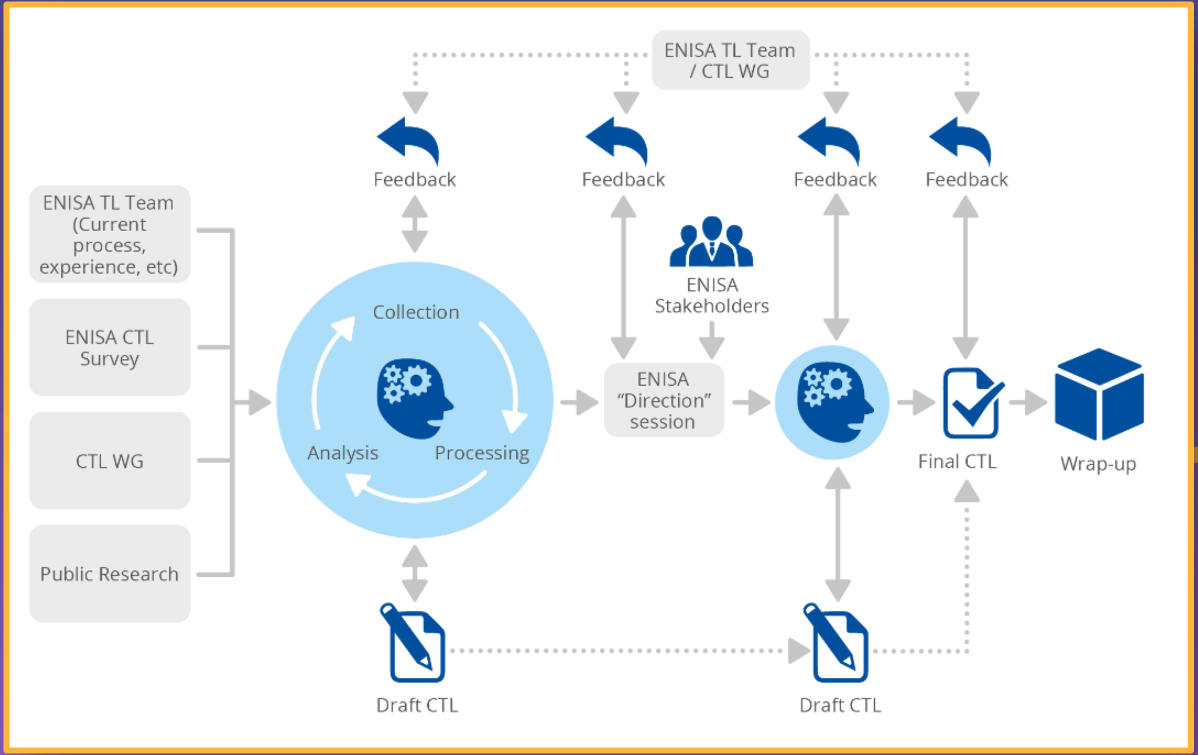


Source: https://paintbynumberspro.com/printable-painting-by-numbers/

- □ Horizontal
- □ Thematic
- □ Sectorial

#2, Applying a process is harder than it seems

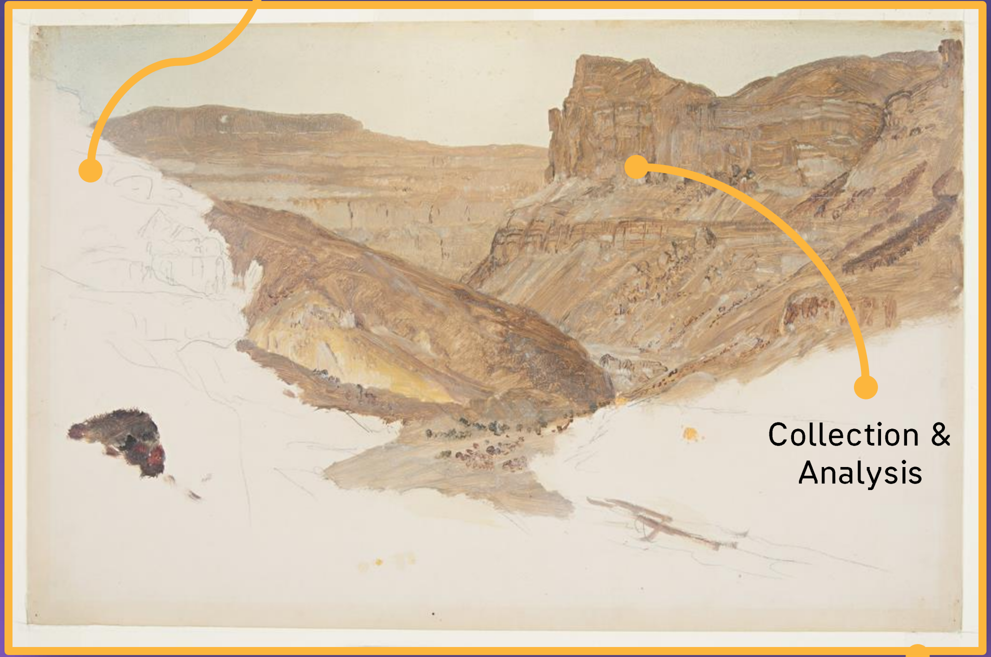
ENISA's methodology



https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

Individual entity

Intelligence requirements



Collection & Analysis

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

Dissemination

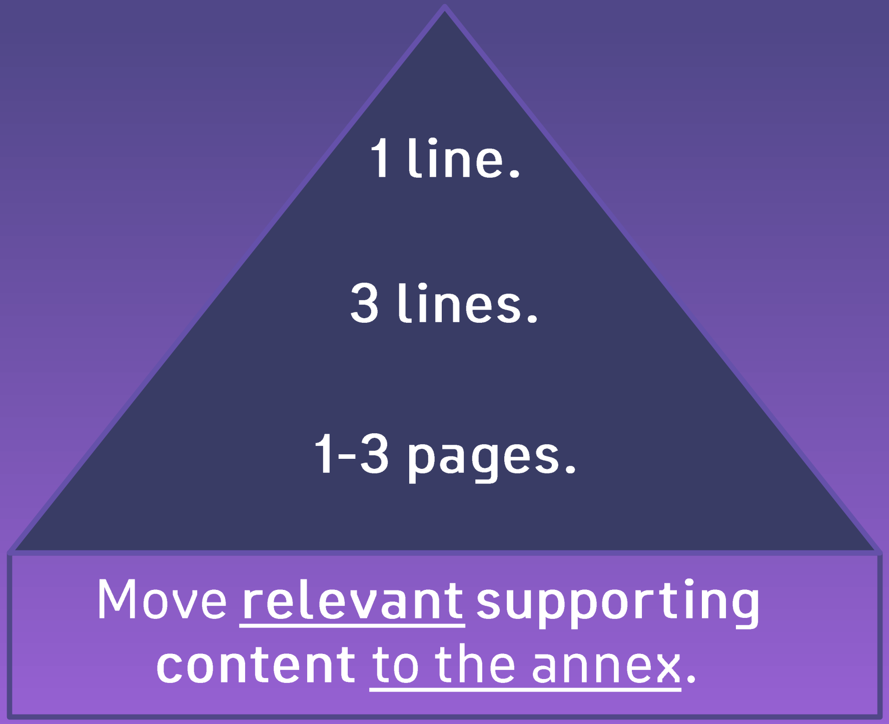
@gertjanbruggink

#3, Considering audiences is crucial for success

- **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.



1 line.

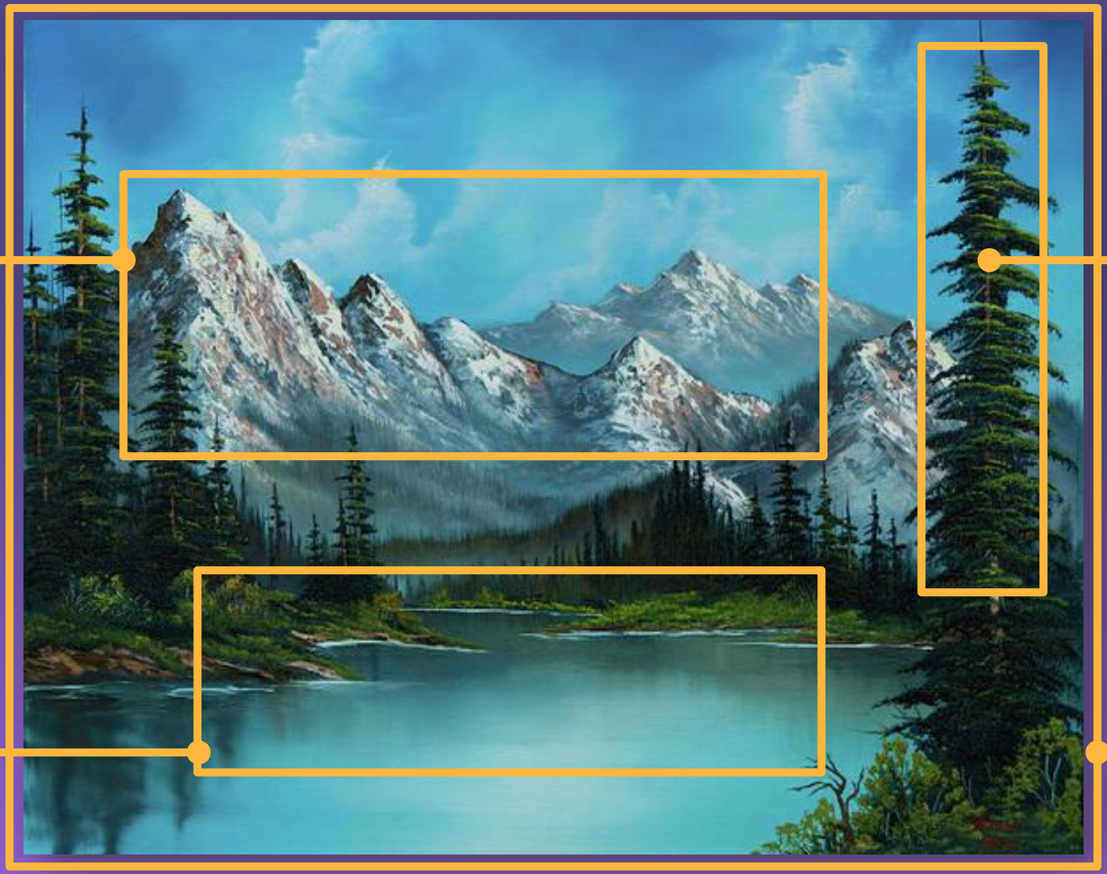
3 lines.

1-3 pages.

Move <u>relevant</u> supporting content <u>to the annex</u>.

GJ's 'Bottom-Line-Up-Front' Pyramid

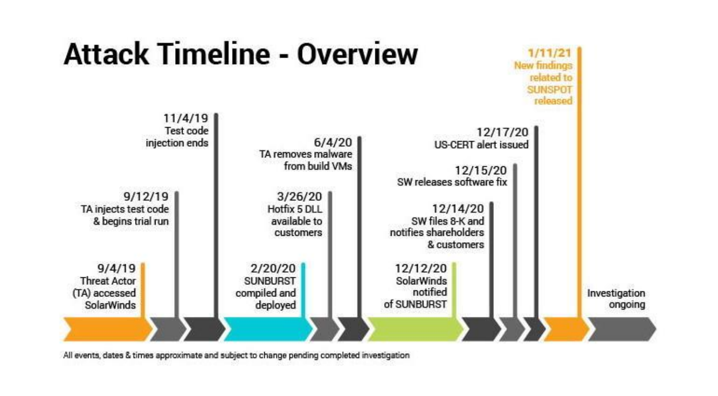
#4, Constantly improve your format on feedback



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

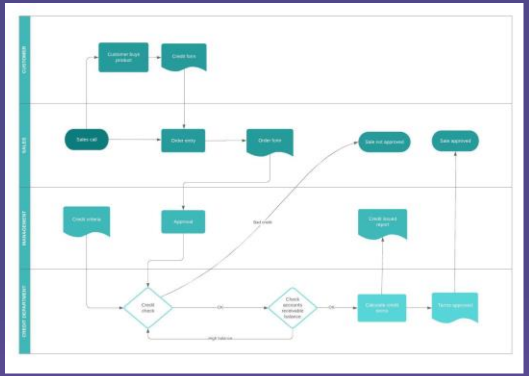
#5, Visualizations make your life easier

Timelines



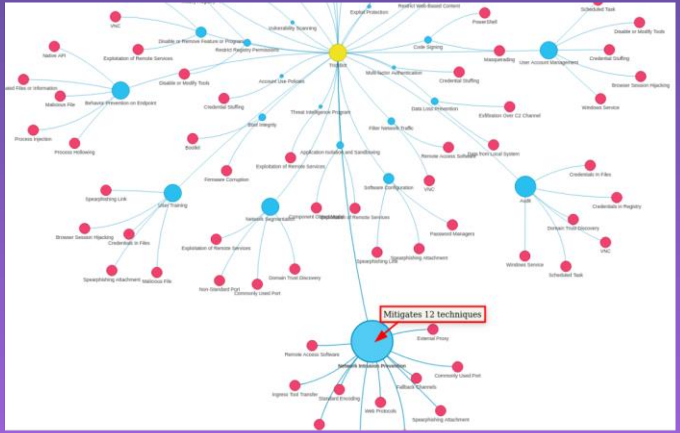
Source: https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/

Flows



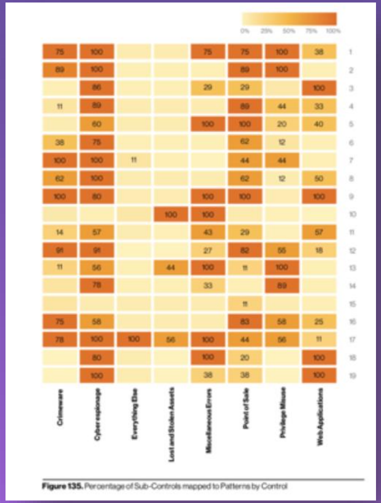
Source:
https://d2slcw3kip6qmk.cloudfront.net/marketing/pages/consideration-page/Business-Process-FlowTemplate.jpeg

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


0%
25%
50%
75%
100%

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

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

Do’s and don'ts

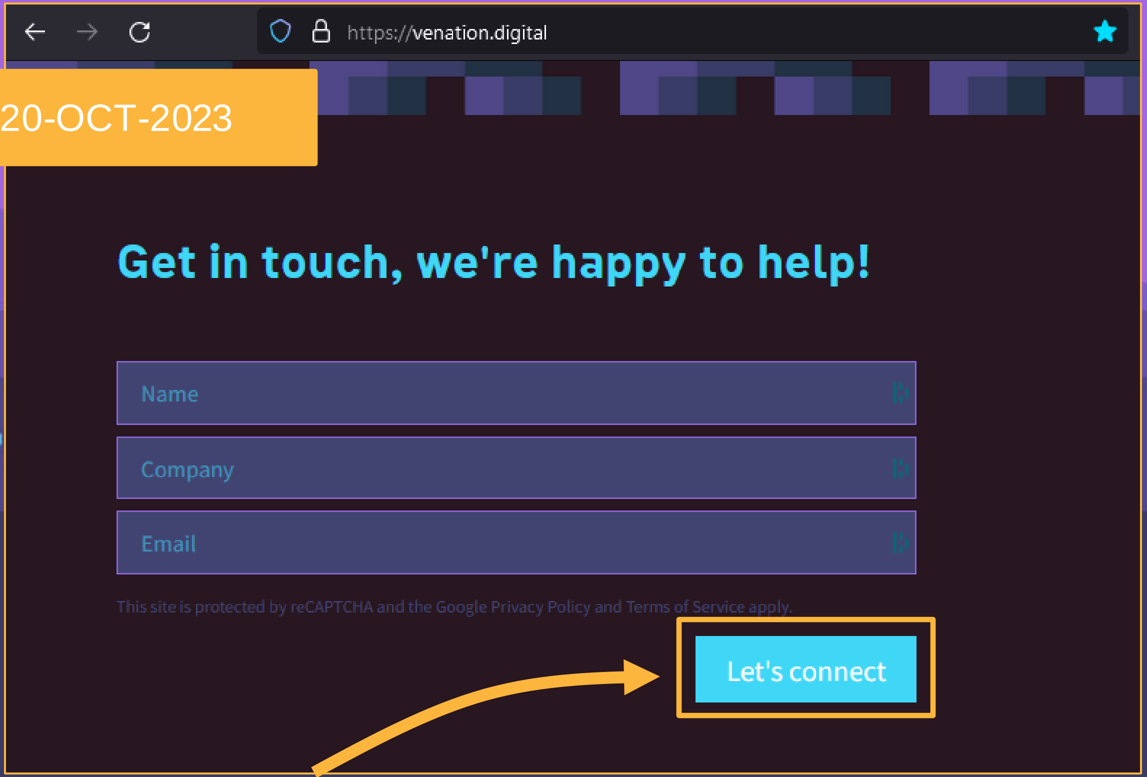
👎

- 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!



20-OCT-2023

Get in touch, we're happy to help!

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Gert-Jan Bruggink

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

Sign up for our free
‘Build Your Own Threat Landscape’
workshop materials via
www.venation.digital

Next available workshop:
6-NOV-2023 @ FIRST CTI 2023