



Monday 🌧️

Tuesday ☁️

Wednesday 🌧️

Thursday ☀️

Friday ☀️

Applied forecasting

Using forecasting techniques to anticipate cyber threats

Gert-Jan Bruggink

SANS CTI Summit 2022

27 January 2022



Why am I here?

**What do people
think it is?**



Image source: <https://www.takemetothefortune.com/wp-content/uploads/2021/09/fortune-teller.jpg>

**Value
proposition**



Image source: <https://pestleanalysis.com/wp-content/uploads/2016/05/strategic-planning-process.jpg>

Example



Great read & quoted source: <https://hbr.org/amp/2022/01/how-corporate-intelligence-teams-help-businesses-manage-risk> by Paul R. Kolbe and Maria Robson Morrow

How bout them cybers?



Who am I?






Gert-Jan Bruggink

cyber threat cartographer

&

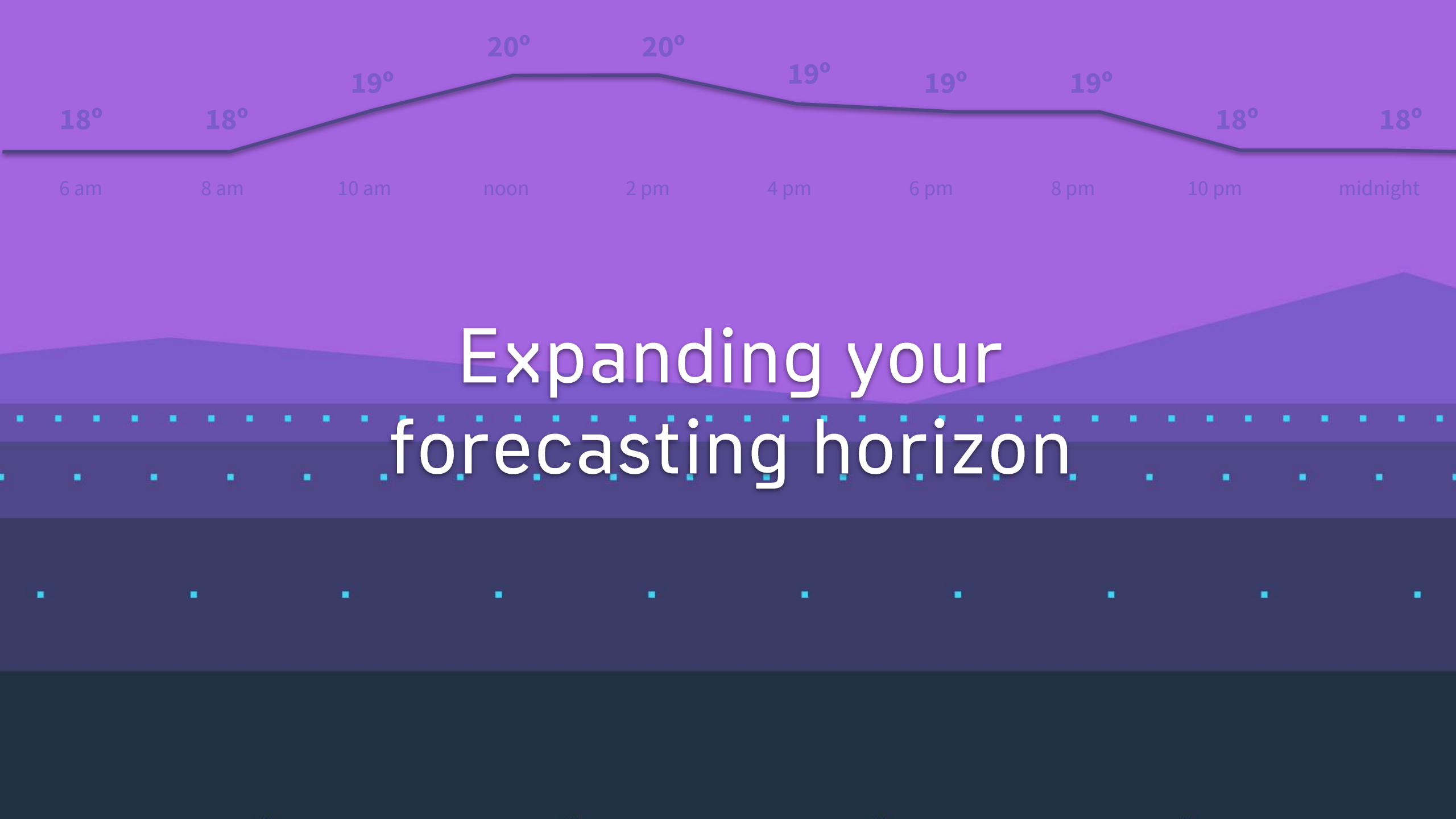
founder Venation

10+ InfoSec.
Financial services, high tech, manufacturing and governmental.
Cyber threat intelligence (CTI) based risk management.
Intelligence-led Red Teaming.
Capability building & leadership.
Strategic change through (CTI, SOC & Cyber) transformation programs.
Father x 2, Entrepreneurship, Gaming, Painting, Lego, Meme's.

 [@gertjanbruggink](https://twitter.com/gertjanbruggink)
 github.com/gertjanbruggink
 [/gertjanbruggink](https://www.linkedin.com/in/gertjanbruggink)

What am I going to talk about?

- ✓ How are these products **created and used** in the private sector?
- ✓ What **adds value** in the private sector context ?
- ✓ Do we have what it takes to become **‘proactive’**?



Expanding your forecasting horizon

Different shades of forecasting

- Prediction vs forecasting
- Forecasting vs ‘super forecasting’
- Forecasting vs ‘nowcasting’

Already an
industry
challenge!

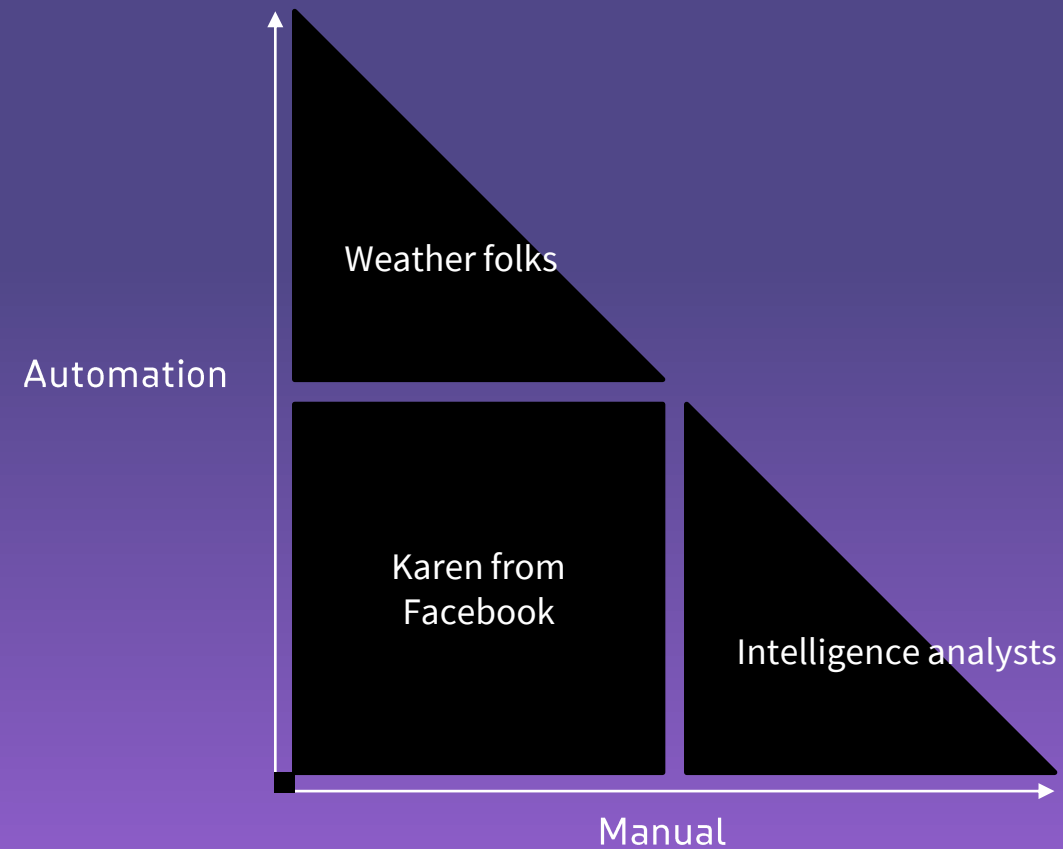


#dartthrowinginfosecchimp

Image source: Dart throwing chimp image: <https://www.reuters.com/>

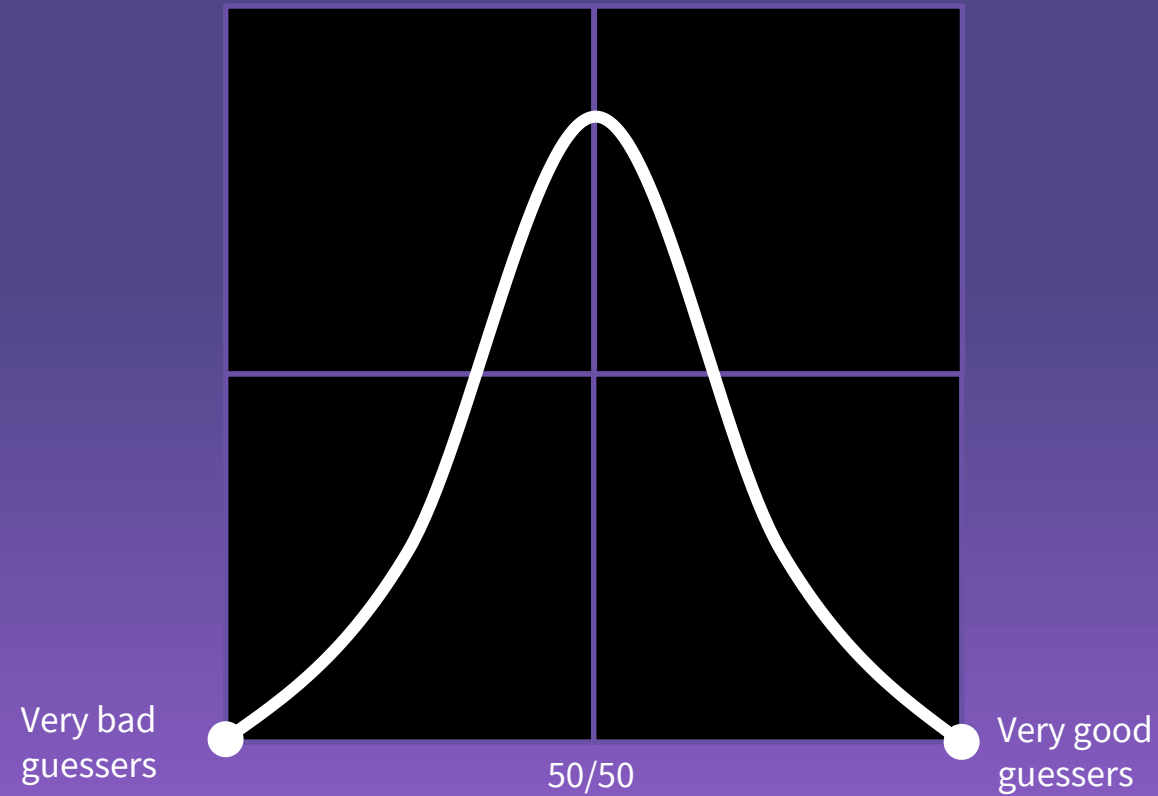


Who actually does forecasting?





Forecasting: luck or skill?



Number of correct guesses

Coin-toss game

Most used forecasting analysis techniques

Qualitative

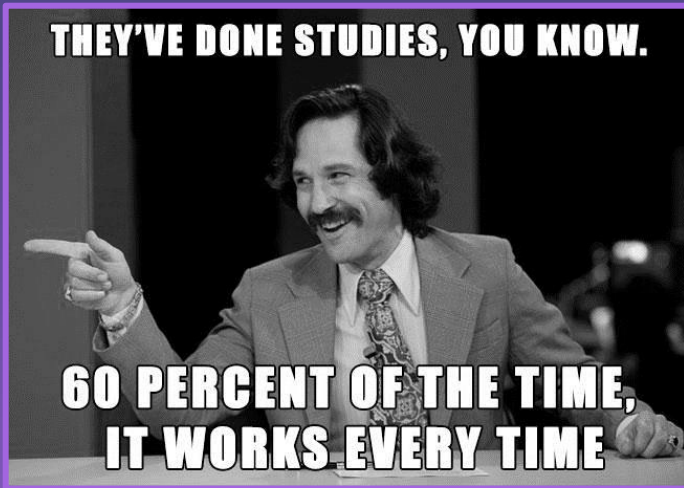


Image source:
<https://www.quotemaster.org/images/77/779c55ba7e7ca2c2728df842b4fd49df.jpg>

Quantitative

Time series analysis and projection

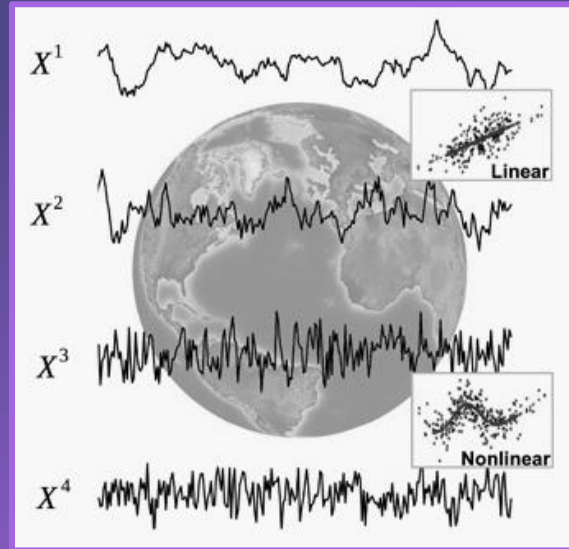


Image source:
<https://advances.sciencemag.org/content/advances/5/11/eaau4996/F1.large.jpg>

Causal models

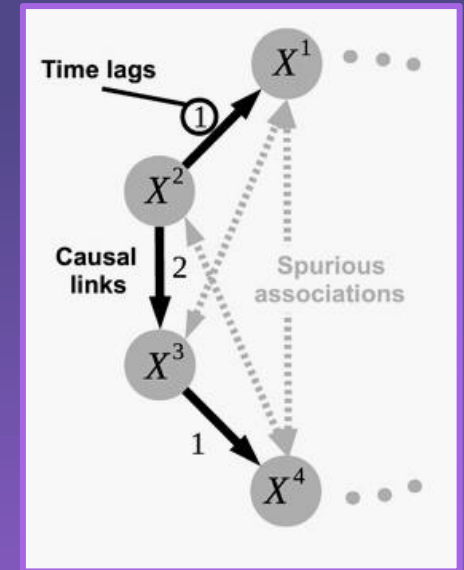
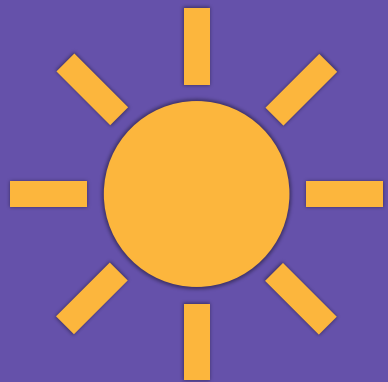


Image source:
<https://advances.sciencemag.org/content/advances/5/11/eaau4996/F1.large.jpg>



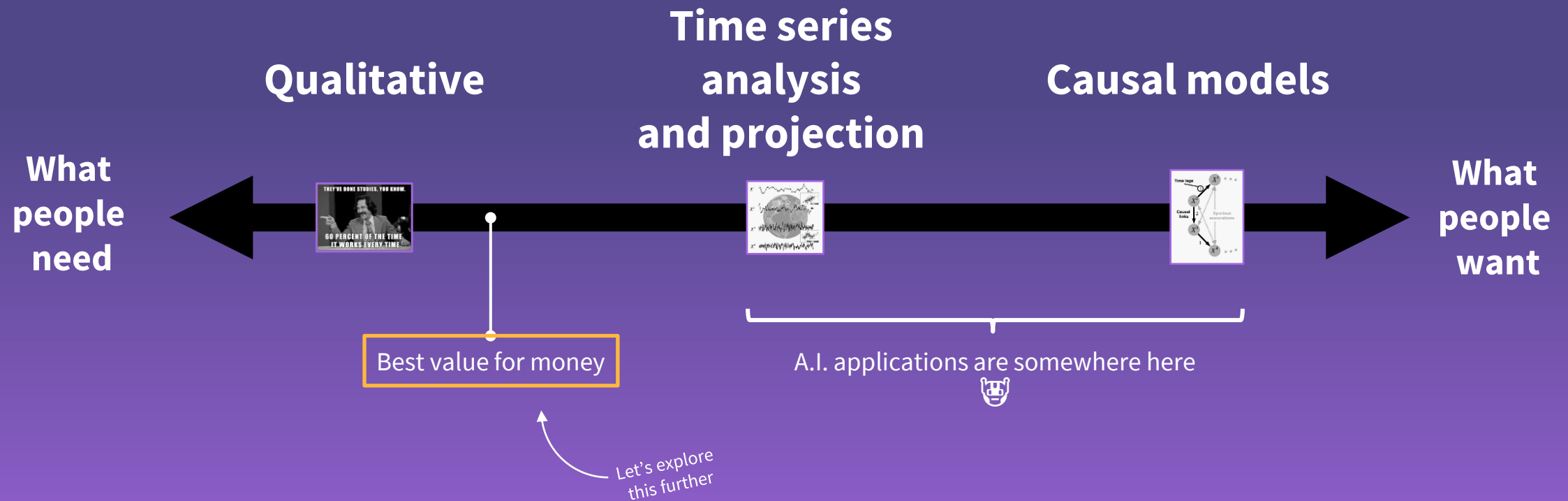
San Francisco

Sunny

22° / 31°

The added value of forecasting in the private sector

Applications in the private sector



Structured analytical technique ‘spirit guidance’

Ways of
grouping them

Purpose

- Diagnostic
- Contrarian
- Imaginative

Purists

- Decomposition and Visualization
- Indicators, Signposts, Scenarios
- Challenging Mindsets
- Hypothesis Generation and Testing
- Group Process Techniques

- Key assumptions check
- Decision support
- Cone of Plausibility
- **Scenario planning**
- Indicators & warnings
- Analysis of competing hypo
- Challenge analysis

Pro tip 📖

Grab ‘Structured Analytic Techniques for Intelligence Analysis’ by Randolph H. Pherson and Richards Heuer – it’s still useful.



Applying a 'SAT' in practice

How you can do 'scenario planning' to forecast threats and structure them as scenarios:

- | | | |
|----|--|---|
| 1 | Schedule quarterly session: do it mid quarter so you benefit the next one. | 'Periodic session' (checks audit box) |
| 2 | Determine a scope: select company, function, etc. | Explicit selection on focus, combine with #1 |
| 3 | Pestle analysis*: frame current understanding of your company or industry. | Establish your industry baseline |
| 4 | Breakdown drivers & assumptions: together with your team, virtual or physical | Track & monitor |
| 5 | Research scenarios: use 'scenario planning' SAT, visualize using a matrix. | Team exercises & fun potential |
| 6 | Create draft set of scenario's: Establish baseline, plausible and wildcard scenarios. | Team exercises & fun potential |
| 7 | Detail scenario's: Try exploring direct lines from high-level narrative to low-level procedures. | Establish a narrative for all parts of your org |
| 8 | Present & share: make sure people are aware of the exercise. | Stakeholder management: leadership |
| 9 | Test & validate: Select specific scenario's and test them! | Risk management |
| 10 | Bonus: identify indicators for warnings, monitor accordingly. | Proactive security posture |

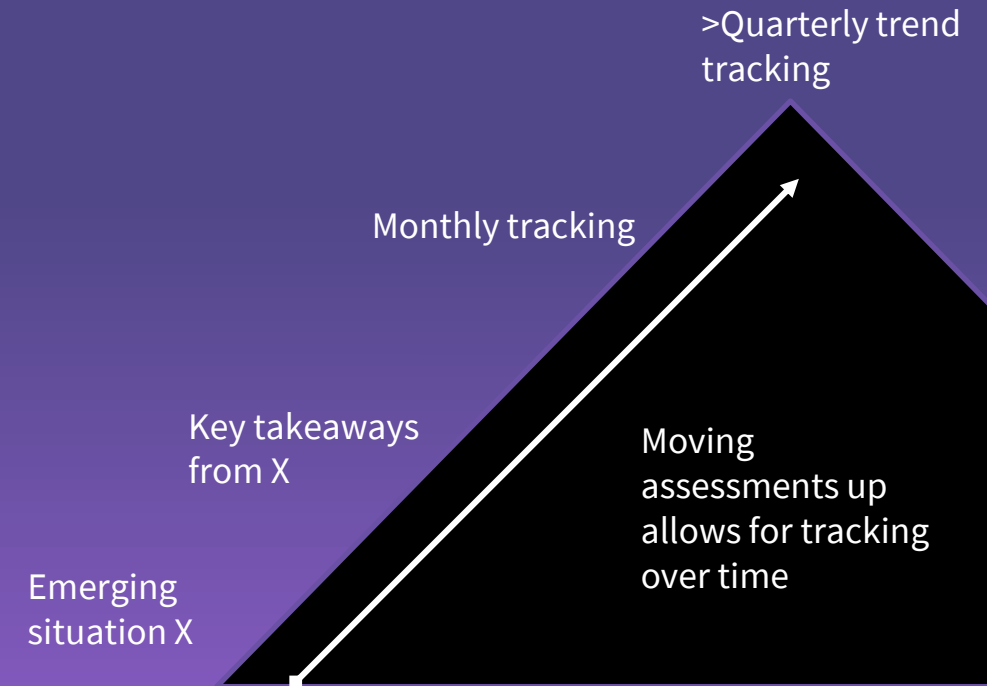
Added
Value



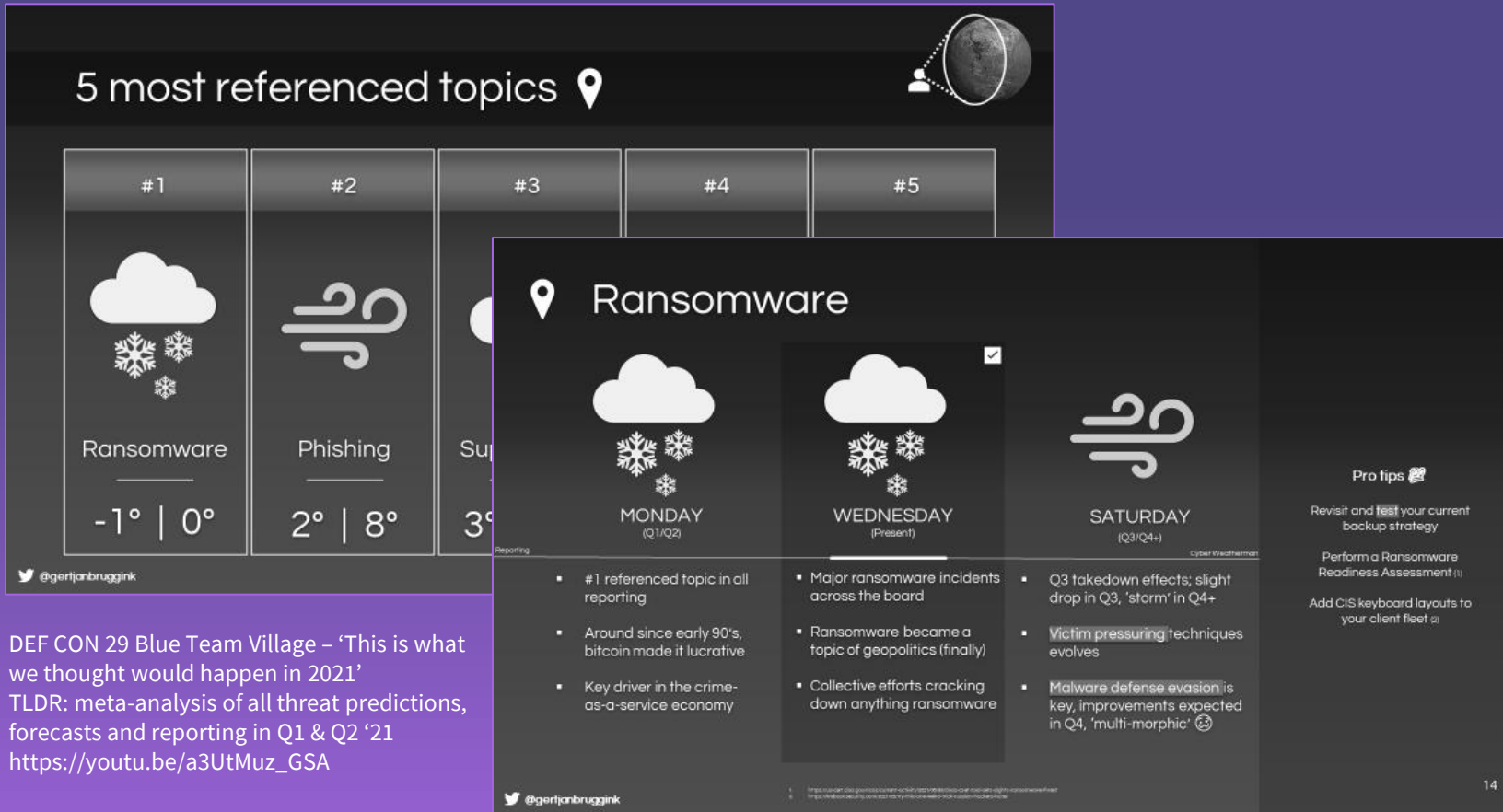
After your analysis, you make assessments

- Forecasting assessments substantiate uncertainty
- For example:

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



If you don't have priority on analysis; look for the 'meta'



DEF CON 29 Blue Team Village – 'This is what we thought would happen in 2021'
TLDR: meta-analysis of all threat predictions, forecasts and reporting in Q1 & Q2 '21
https://youtu.be/a3UtMuz_GSA

- Spotting pros and cons in publishers (source & collection management)
- Identifying trends and actioning them (analysis & dissemination)
- Improving the structure of deliverables (deliverable templating)

Everyone wants to do forecasting, not everyone wants to do the work

!! It takes people and skill.

!! It takes time to do this right.

!! You might not find the conclusions valuable.



Do we have what it takes?



Explicit consideration of capability and intent helps reduce grey areas

- Risk = Impact x likelihood
- Risk = Impact x likelihood (threat x asset x vulnerability)
- **Risk = Impact x likelihood x threat (capability x intent x opportunity)**
- Risk = Threat x vulnerability/capacity
- Risk = Impact x likelihood

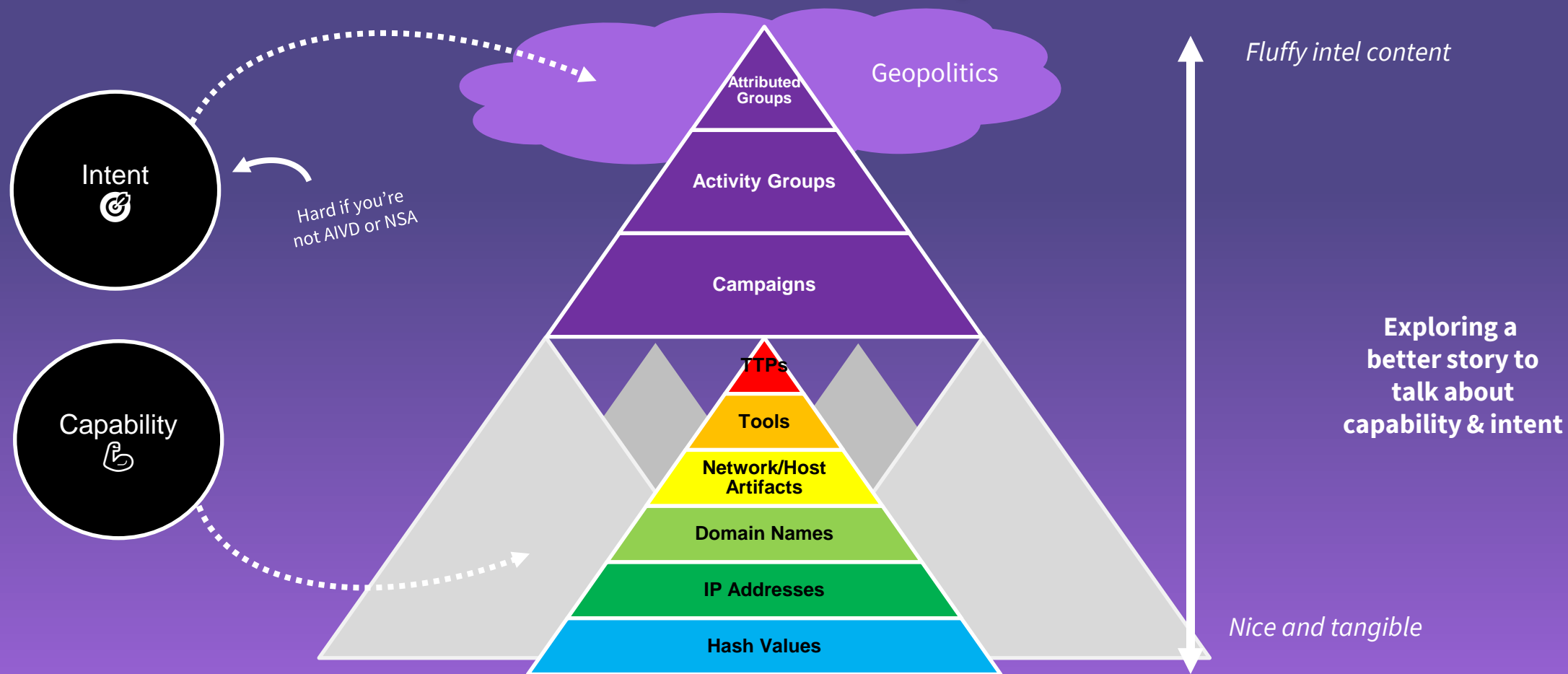
← Risk management
multiverse

Pro tip 📖

Seek common 'risk management' ground, by aligning on data both of you are using.



Expanding perspective using traditional data points

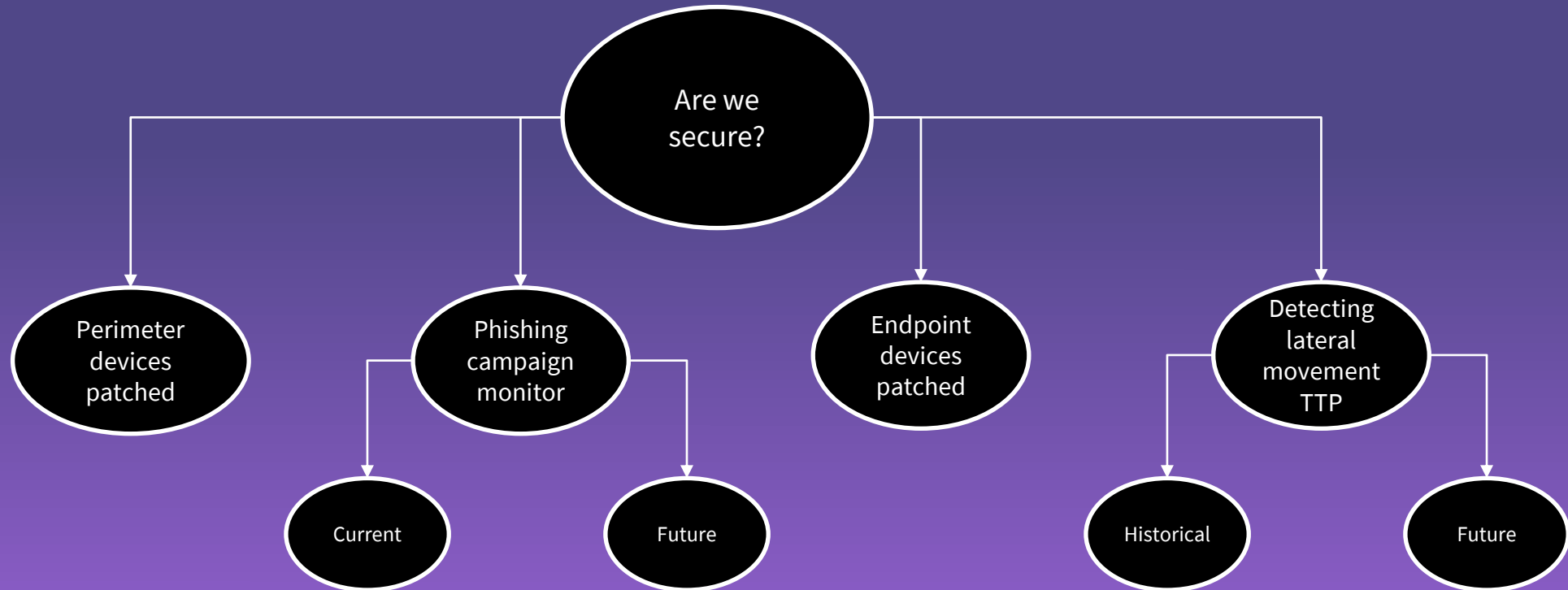


Extending the 'Pyramid of pain'

Stop asking big questions, start asking small questions

From this:

To this:



Bayesian question clustering

Purpose driven
organizations are
good at this



Understand that any ‘forward looking’ questions come at a cost

Accuracy: skill/time

Accuracy	
Short term (0–3 months)	Fair to very good
Medium term (3 months–2 years)	Fair to very good
Long term (2 years & up)	Fair to very good

Cost: time/technology

Cost of forecasting*	
With a computer	\$2,000+
Is calculation possible without a computer?	Yes

BASIC FORECASTING TECHNIQUES			
Technique	A. Qualitative Methods		
	1. Delphi Method	2. Market Research	3. Panel Consensus
Description	A panel of experts is interrogated by a sequence of questionnaires in which the responses to one questionnaire are used to produce the next questionnaire. Any set of information available to some experts and not others is thus passed on to the others, enabling all the experts to have access to all the information for forecasting. This technique eliminates the bandwagon effect of majority opinion.	The systematic, formal, and conscious procedure for evolving and testing hypotheses about real markets.	This technique is based on the assumption that several experts can arrive at a better forecast than one person. There is no secrecy, and communication is encouraged. The forecasts are sometimes influenced by social factors, and may not reflect a true consensus.
Accuracy	Short term (0–3 months) Fair to very good Medium term (3 months–2 years) Fair to very good Long term (2 years & up) Fair to very good	Excellent Good Fair to good	Poor to fair Poor to fair Poor
Identification of turning points	Fair to good	Fair to very good	Poor to fair
Typical applications	Forecasts of long-range and new-product sales, forecasts of margins.	Forecasts of long-range and new-product sales, forecasts of margins.	Forecasts of long-range and new-product sales, forecasts of margins.
Data required	A coordinator issues the sequence of questionnaires, editing and consolidating the responses.	As a minimum, two sets of reports over time. One needs a considerable collection of market data from questionnaires, surveys, and time series analyses of market variables.	Information from a panel of experts is presented openly in group meetings to arrive at a consensus forecast. Again, a minimum is two sets of reports over time.
Cost of forecasting*	With a computer \$2,000+ Is calculation possible without a computer? Yes	\$5,000+ Yes	\$1,000+ Yes
Time required to develop an application & make a forecast	2 months+	3 months+	2 weeks +
References	North & Pyke, “‘Probes’ of the Technological Future,” HBR May–June 1969, p. 68.	Bass, King & Pessemier, <i>Applications of the Sciences in Marketing Management</i> (New York, John Wiley & Sons, Inc., 1968).	—

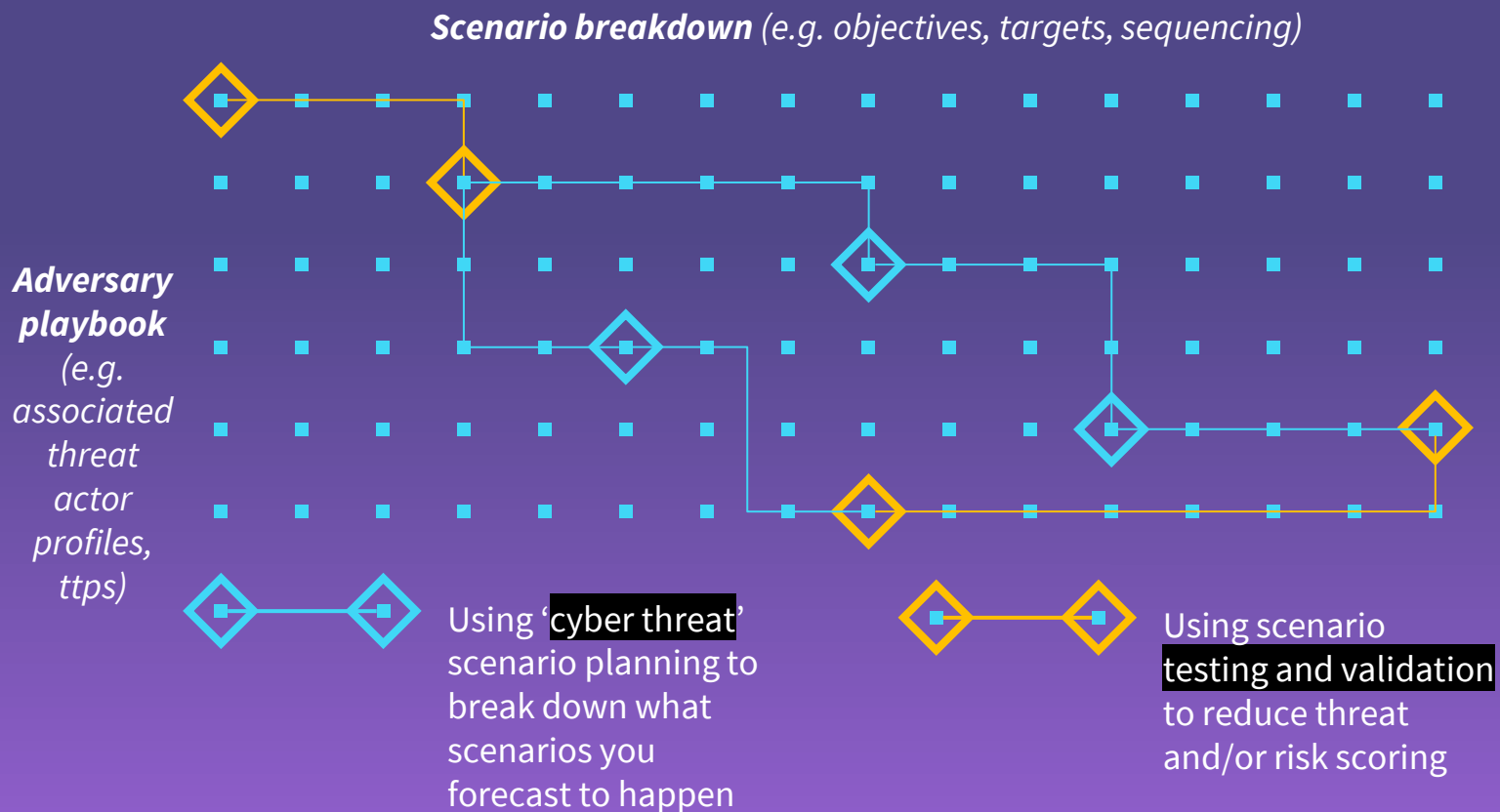
1971’ example of how we compared techniques at the time

50 years ago lol

*These estimates are based on our own experience, using this machine configuration: an IBM 360-40, 256 K system and a Univac 1108 Time-sharing System, together with such smaller equipment as GE Time-sharing and IBM 360-30's and 1130's.



Explore a scenario-based approach



```
1 # Title, detailing what happens in this scenario, by whom, and directed by
2 # what objective
3
4 ## Overview
5
6 **Identifier:** YEAR-MONTH-NAME (e.g. 202110-SCENARIO_HAPPENS_ABC)
7
8 **Timestamp:** YEAR-MONTH-DAY - time (e.g. 2021-11-11, 10:00)
9
10 **Author(s):** [Venation](https://venation.digital/)
11
12 **Industry Tagging:**
13 'Financial Services'
14 'Customer banking'
15 'Maritime'
16 'High Tech'
17 'Semiconductors'
18
19 **Scenario Tagging:**
20 'APT28'
21 'Mobile malware'
22 'Watering hole'
23 'Application access token'
24
25 <!--
26 Tags for each scenario are listed here
27 analyze scenarios. For example to do
28 tagging should consist of key activity
29 vulnerability' or 'ransomware'
30 -->
31
32 ## Scenario breakdown
33
34 **Objective(s):**
35
36 Any_relevant_input_is_detailed_here
37
38 **Summary:**
39
40 Any_relevant_input_is_detailed_here
41
42 <!--
43 Detailing the most likely objective(s)
44 than one objective, items shall be the
45 most-likely to least likely.
46 -->
47
48 **Scenario sequence:**
49
50 1. Step - Reconnaissance
51 2. Step - Initial access
52 3. Step - Lateral movement
53
54 Adversary playbook
55
56 **Considerations:**
57
58 Any_relevant_input_is_detailed_here
59
60 Associated threat actor profile:
61
62 **Functions and/or systems targeted:**
63
64 Any_relevant_input_is_detailed_here
65
66 <!--
67 The summary describes the why, how, of
68 3 paragraphs, aligned with the why-how
69 text per paragraph. Rows of text with
70 voice.
71 -->
72
73 TTP breakdown:
74
75 <table>
76 <thead>
77 <tr>
78 <th>Tactic ID</th>
79 <th>Tactic ID</th>
80 <th>Technique ID</th>
81 <th>Technique</th>
82 <th>Procedure(s)</th>
83 <th>Detection Opportunity</th>
84 </tr>
85 </thead>
86 <tbody>
87 <tr>
88 <td>APT28</td>
89 <td>State-sponsored entity</td>
90 <td>High</td>
91 <td>High</td>
92 <td>TBD</td>
93 </tr>
94 </tbody>
95 </table>
96
97 <!--
98 Summary or
99 additional
100 phishing
101 operations.
102 -->
```

Title, detailing what happens in this scenario, by whom, and directed by what objective

Overview

Identifier: YEAR-MONTH-NAME (e.g. 202110-SCENARIO_HAPPENS_ABC)

Timestamp: YEAR-MONTH-DAY - time (e.g. 2021-11-11, 10:00)

Author(s): Venation

Industry Tagging: 'Financial Services' 'Customer banking' 'Maritime' 'High Tech' 'Semiconductors'

Scenario Tagging: 'APT28' 'Mobile malware' 'Watering hole' 'Application access token'

Scenario breakdown

Objective(s):

Any_relevant_input_is_detailed_here

Summary:

Any_relevant_input_is_detailed_here

Functions and/or systems targeted:

Any_relevant_input_is_detailed_here

Scenario sequence:

1. Step - Reconnaissance
2. Step - Initial access
3. Step - Lateral movement

Adversary playbook

Considerations:

Any_relevant_input_is_detailed_here

Associated threat actor profile:

Name	Category	Capability	Intent	Comments
APT28	State-sponsored entity	High	High	TBD

TTP breakdown:

Tactic ID	Tactic ID	Technique ID	Technique	Procedure(s)	Detection Opportunity
					Acquired

Example scenario format, now available via:
<https://github.com/venation-digital/>

Finally, tracking & monitoring your stuff



Source: <https://www.youtube.com/watch?v=QaK0NK7dmmU&t=2582s>

- Reviewing your forecast assessments periodically
- Benchmarking & comparing forecasts

Pro tip 

Haute cuisine for Excel lovers & 'indicators & warnings' champions alike!



Recap & course of action

- You need basics (really).
- Give forecasting actual priority.
- Small steps are big steps in the private sector .

Contemplate this today

- ✓ Schedule your next scenario planning session (slide 13).
- ✓ Take a moment to do the analysis (slide 14, 20, 23).
- ✓ Use the scenario structure to frame your results and action it (slide 19, 22).

Action this tomorrow

Let's continue the discussion!

Want to build a weather forecast?

Gert-Jan Bruggink

#cyberweatherman



@gertjanbruggink



/gertjanbruggink

You can find the references made throughout the presentation after this slide!

Special thanks to:
Sherman, Peter, Sophie, Rick

References

Slide 2	How Corporate Intelligence Teams Help Businesses Manage Risk	https://hbr.org/amp/2022/01/how-corporate-intelligence-teams-help-businesses-manage-risk
Slide 6, 8, 20	Superforecasting: The Art and Science of Prediction	https://www.amazon.com/Superforecasting-Science-Prediction-Philip-Tetlock/dp/0804136718
Slide 9, 11	Introduction to causal models	https://www.youtube.com/watch?v=vGcWJcgY-MY https://www.youtube.com/watch?v=mbt6W5E1m9Y
Slide 9, 11	Causal inference, causal models	https://www.youtube.com/watch?v=AuZu0L0PEgk
Slide 9, 11	Time Series Forecasting for Beginners	https://towardsdatascience.com/time-series-essentials-fe6727ab6a94 https://www.youtube.com/watch?v=chp71nEc320
Slide 12	Conventional Intelligence Analysis in Cyber Threat Intelligence - CTI Summit 2017	https://www.youtube.com/watch?v=jzHw8lkocXA
Slide 12	Analytic Tradecraft in the Real World - SANS CTI Summit 2019	https://www.youtube.com/watch?v=MWJZsW9HooY&list=PLfouvuAjsTpTrqyys__cMrkA83-gAiFokE&index=8
Slide 12, 13	There Is MOAR To Structured Analytic Techniques Than Just ACH! - SANS CTI Summit 2018	https://www.youtube.com/watch?v=PtYWVzY2Ves&list=PLfouvuAjsTpPiPz2QUuiC73K5xzyDgPnM&index=11
Slide 15	DEF CON 29 Blue Team Village – ‘This is what we thought would happen in 2021’	https://youtu.be/a3UtMuz_GSA
Slide 20	Bayesian cluster analysis	https://projecteuclid.org/journals/bayesian-analysis/volume-13/issue-2/Bayesian-Cluster-Analysis--Point-Estimation-and-Credible-Balls-with/10.1214/17-BA1073.pdf